(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－6608

(43)公開日　平成９年(1997)１月10日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	9/06	５５０		Ｇ０６Ｆ	9/06	５５０Ｈ
	12/14	３２０			12/14	３２０Ｆ

審査請求　未請求　請求項の数19　ＯＬ　（全 26 頁）

(21)出願番号　特願平7－156538

(22)出願日　平成７年(1995)６月22日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　大森　基司
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　舘林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

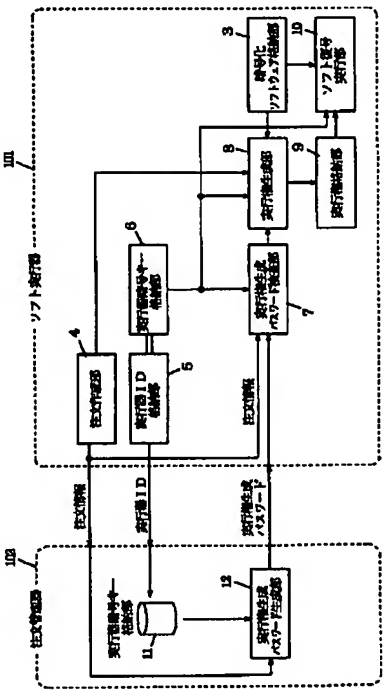
(74)代理人　弁理士　小笠原　史朗

(54)【発明の名称】　ソフトウェア保護システム

(57)【要約】　（修正有）

【目的】　ソフトの実行権を通信路を用いて獲得する場合、通信路上のデータ、特にランダムな値の桁数を削減する。

【構成】　ソフト実行器１０１は、実行器ＩＤおよび注文情報を生成し、これらを注文管理器１０２に送付することにより、ソフトウェアの注文を行なう。注文管理器１０２は、受け取った注文情報と、実行ＩＤに対応する実行器秘密情報とに依存した情報である実行権生成パスワードを生成し、ソフト実行器１０１に送付する。ソフト実行器１０１は、この実行権生成パスワードが、注文管理器１０２に先に送付した注文情報や、自分自身の実行器秘密情報と整合している否かを判断し、整合している場合は、注文情報に対応したソフトウェアの実行権を生成し、当該ソフトウェアを実行する。



【特許請求の範囲】
【請求項１】　提供されたソフトウェアを実行する１つ以上のソフト実行器と、各ソフト実行器と通信経路を介して接続され、かつ各ソフト実行器から受けたソフトウェアの注文を管理する注文管理器とを備えたソフトウェア保護システムであって、
各前記ソフト実行器は、
固有の実行器ＩＤを格納する実行器ＩＤ格納手段と、
固有の実行器秘密情報を格納する第１の秘密情報格納手段と、
１つ以上のソフトウェアの実行権の注文情報を作成して蓄積保持する注文作成手段とを含み、
前記実行器ＩＤおよび前記注文情報は、前記通信路を介して前記注文管理器に送付され、
前記注文管理器は、
各前記ソフト実行器に格納された全ての実行器秘密情報を格納する第２の秘密情報格納手段と、
前記ソフト実行器から受け取った実行器ＩＤに対応する実行器秘密情報を前記第２の秘密情報格納手段から獲得し、この獲得した実行器秘密情報およびソフト実行器から受け取った注文情報に依存した実行権生成パスワードを生成する実行権生成パスワード生成手段とを含み、
前記実行権生成パスワードは、前記通信路を介して前記ソフト実行器に送付され、
各前記ソフト実行器は、さらに前記注文作成手段に蓄積保持された注文情報と、前記第１の秘密情報格納手段に格納された実行器秘密情報とを用いて、前記注文管理器から受け取った実行権生成パスワードの正当性を検査する実行権生成パスワード検査手段と、
前記実行権生成パスワード検査手段による検査の結果、前記実行権生成パスワードの正当性が確認されたときに、前記注文作成手段に蓄積保持された注文情報に基づいて、注文されたソフトウェアの実行権を生成する実行権生成手段と、
前記実行権が存在するソフトウェアを、当該実行権に示される実行条件に従って実行するソフト実行手段とを含む、ソフトウェア保護システム。
【請求項２】　前記実行権生成パスワード生成手段は、前記ソフト実行器から受け取った注文情報と、前記第２の秘密情報格納手段から獲得した実行器秘密情報とを、出力が入力ビットのすべてに関係するようなデータ圧縮関数に入力し、このデータ圧縮関数の出力結果を、前記実行権生成パスワードとして出力し、
前記実行権生成パスワード検査手段は、前記注文作成手段に蓄積保持された注文情報と、前記第１の秘密情報格納手段に格納された実行器秘密情報とを、前記実行権生成パスワード生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、その出力結果が注文管理器から受け取った実行権生成パスワードと一致したとき、当該実行権生成パスワードが正当であると判断することを特徴とする、請求項１に記載のソフトウェア保護システム。
【請求項３】　前記注文管理器は、公開鍵署名方式に用いられる秘密情報を格納する第３の秘密情報格納手段をさらに含み、
前記実行権生成パスワード生成手段は、前記第３の秘密情報格納手段に格納された秘密情報と、前記第２の秘密情報格納手段から獲得した実行器秘密情報と、前記ソフト実行器から受け取った注文情報と用いて、公開鍵署名方式によってデジタル署名された実行権生成パスワードを生成し、
前記ソフト実行器は、前記公開鍵署名方式に用いられる秘密情報に対応した公開情報を格納する公開情報格納手段をさらに含み、
前記実行権生成パスワード検査手段は、前記公開情報格納手段に格納された公開情報と、前記注文作成手段に蓄積保持された注文情報と、前記第１の秘密情報格納手段に格納された実行器秘密情報とを用いて、前記公開鍵署名方式に対応した署名確認方式によって、前記注文管理器から受け取った実行権生成パスワードの正当性を検査することを特徴とする、請求項１に記載のソフトウェア保護システム。
【請求項４】　提供されたソフトウェアを実行する１つ以上のソフト実行器と、各ソフト実行器と通信経路を介して接続され、かつ各ソフト実行器から受けたソフトウェアの注文を管理する注文管理器とを備えたソフトウェア保護システムであって、
各前記ソフト実行器は、
固有の実行器ＩＤを格納する実行器ＩＤ格納手段と、
固有の実行器秘密情報を格納する第１の秘密情報格納手段と、
１つ以上のソフトウェアの実行権の注文情報を作成して蓄積保持する注文作成手段と、
前記注文作成手段で注文情報が作成される毎に変化する変化値を生成して蓄積保持する変化値生成手段とを含み、
前記実行器ＩＤ，前記注文情報および前記変化値は、前記通信路を介して前記注文管理器に送付され、
前記注文管理器は、
各前記ソフト実行器に格納された全ての実行器秘密情報を格納する第２の秘密情報格納手段と、
前記ソフト実行器から受け取った実行器ＩＤに対応する実行器秘密情報を前記第２の秘密情報格納手段から獲得し、この獲得した実行器秘密情報，ソフト実行器から受け取った注文情報および変化値に依存した実行権生成パスワードを生成する実行権生成パスワード生成手段とを含み、
前記実行権生成パスワードは、前記通信路を介して前記ソフト実行器に送付され、
各前記ソフト実行器は、さらに前記注文作成手段に蓄積

保持された注文情報と、前記変化値生成手段に蓄積保持された変化値と、前記第１の秘密情報格納手段に格納された実行器秘密情報とを用いて、前記注文管理器から受け取った実行権生成パスワードの正当性を検査する実行権生成パスワード検査手段と、
前記実行権生成パスワード検査手段による検査の結果、前記実行権生成パスワードの正当性が確認されたときに、前記注文作成手段に蓄積保持された注文情報に基づいて、注文されたソフトウェアの実行権を生成する実行権生成手段と、
前記実行権が存在するソフトウェアを、当該実行権に示される実行条件に従って実行するソフト実行手段とを含む、ソフトウェア保護システム。
【請求項５】　前記実行権生成パスワード生成手段は、前記ソフト実行器から受け取った注文情報および変化値と、前記第２の秘密情報格納手段から獲得した実行器秘密情報とを、出力が入力ビットのすべてに関係するようなデータ圧縮関数に入力し、このデータ圧縮関数の出力結果を、前記実行権生成パスワードとして出力し、
前記実行権生成パスワード検査手段は、前記注文作成手段に蓄積保持された注文情報と、前記変化値生成手段に蓄積保持された変化値と、前記第１の秘密情報格納手段に格納された実行器秘密情報とを、前記実行権生成パスワード生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、その出力結果が注文管理器から受け取った実行権生成パスワードと一致したとき、当該実行権生成パスワードが正当であると判断することを特徴とする、請求項４に記載のソフトウェア保護システム。
【請求項６】　提供されたソフトウェアを実行する１つ以上のソフト実行器と、各ソフト実行器と通信経路を介して接続され、かつ各ソフト実行器から受けたソフトウェアの注文を管理する注文管理器とを備えたソフトウェア保護システムであって、
各前記ソフト実行器は、
固有の実行器ＩＤを格納する実行器ＩＤ格納手段と、
固有の実行器秘密情報を格納する第１の秘密情報格納手段と、
１つ以上のソフトウェアの実行権の注文情報を作成して蓄積保持する注文作成手段と、
前記注文作成手段で注文情報が作成される毎にタイムスタンプを生成して蓄積保持する第１のタイムスタンプ生成手段とを含み、
前記実行器ＩＤおよび前記注文情報は、前記通信路を介して前記注文管理器に送付され、
前記注文管理器は、
前記ソフト実行器から実行器ＩＤおよび注文情報を受け取ると、タイムスタンプを生成する第２のタイムスタンプ生成手段と、
各前記ソフト実行器に格納された全ての実行器秘密情報を格納する第２の秘密情報格納手段と、
前記ソフト実行器から受け取った実行器ＩＤに対応する実行器秘密情報を前記第２の秘密情報格納手段から獲得し、この獲得した実行器秘密情報と、ソフト実行器から受け取った注文情報と、前記第２のタイムスタンプ生成手段で生成されたタイムスタンプとに依存した実行権生成パスワードを生成する実行権生成パスワード生成手段とを含み、
前記実行権生成パスワードは、前記通信路を介して前記ソフト実行器に送付され、
各前記ソフト実行器は、さらに前記注文作成手段に蓄積保持された注文情報と、前記第１のタイムスタンプ生成手段に蓄積保持されたタイムスタンプと、前記第１の秘密情報格納手段に格納された実行器秘密情報とを用いて、前記注文管理器から受け取った実行権生成パスワードの正当性を検査する実行権生成パスワード検査手段と、
前記実行権生成パスワード検査手段による検査の結果、前記実行権生成パスワードの正当性が確認されたときに、前記注文作成手段に蓄積保持された注文情報に基づいて、注文されたソフトウェアの実行権を生成する実行権生成手段と、
前記実行権が存在するソフトウェアを、当該実行権に示される実行条件に従って実行するソフト実行手段とを含む、ソフトウェア保護システム。
【請求項７】　提供されたソフトウェアを実行する１つ以上のソフト実行器と、各ソフト実行器と通信経路を介して接続され、かつ各ソフト実行器から受けたソフトウェアの注文を管理する注文管理器とを備えたソフトウェア保護システムであって、
各前記ソフト実行器は、
固有の実行器ＩＤを格納する実行器ＩＤ格納手段と、
固有の実行器秘密情報を格納する第１の秘密情報格納手段と、
１つ以上のソフトウェアの実行権の注文情報を作成して蓄積保持する注文作成手段と、
前記注文情報と前記実行器秘密情報に依存した注文認証情報を生成して蓄積保持する注文認証情報生成手段とを含み、
前記実行器ＩＤ，前記注文情報および前記注文認証情報は、前記通信路を介して前記注文管理器に送付され、
前記注文管理器は、
各前記ソフト実行器に格納された全ての実行器秘密情報を格納する第２の秘密情報格納手段と、
前記ソフト実行器から受け取った実行器ＩＤに対応する実行器秘密情報を前記第２の秘密情報格納手段から獲得し、この獲得した実行器秘密情報，ソフト実行器から受け取った注文情報および注文認証情報を用いて、ソフト実行器および注文情報の認証を行い、この認証結果が正当である場合に、当該注文認証情報を注文を識別する注文識別情報として扱う実行器認証手段と、

前記実行器認証手段における認証結果が正当である場合にのみ、前記注文情報および前記注文識別情報に依存した実行権生成パスワードを生成する実行権生成パスワード生成手段とを含み、
前記実行権生成パスワードは、前記注文識別情報と共に、前記通信路を介して前記ソフト実行器に送付され、
各前記ソフト実行器は、さらに前記注文作成手段に蓄積保持された注文情報と、前記注文認証情報生成手段に蓄積保持された注文認証情報とを用いて、前記注文管理器から受け取った実行権生成パスワードの正当性を検査する実行権生成パスワード検査手段と、
前記実行権生成パスワード検査手段による検査の結果、前記実行権生成パスワードの正当性が確認されたときに、前記注文作成手段に蓄積保持された注文情報に基づいて、注文されたソフトウェアの実行権を生成する実行権生成手段と、
前記実行権が存在するソフトウェアを、当該実行権に示される実行条件に従って実行するソフト実行手段とを含む、ソフトウェア保護システム。
【請求項８】　前記注文認証情報生成手段は、前記注文作成手段によって作成された注文情報と、前記第１の秘密情報格納手段に格納された実行器秘密情報とを、出力が入力ビットのすべてに関係するようなデータ圧縮関数に入力し、このデータ圧縮関数の出力結果を、前記注文認証情報として出力し、
前記実行器認証手段は、前記第２の秘密情報格納手段から獲得した実行器秘密情報と、ソフト実行器から受け取った注文情報とを、前記注文認証情報生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、このデータ圧縮関数の出力結果がソフト実行器から受け取った注文認証情報と一致する場合に、注文を行ったソフト実行器および注文情報が正当であることを認証し、
前記実行権生成パスワード生成手段は、前記ソフト実行器から受け取った注文情報および前記注文識別情報を、前記注文認証情報生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、このデータ圧縮関数の出力結果を、前記実行権生成パスワードとして出力し、
前記実行権生成パスワード検査手段は、前記注文作成手段に蓄積保持された注文情報と、前記注文認証情報生成手段に蓄積保持された注文認証情報とを、前記注文認証情報生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、その出力結果が注文管理器から受け取った実行権生成パスワードと一致したとき、当該実行権生成パスワードが正当であると判断することを特徴とする、請求項７に記載のソフトウェア保護システム。
【請求項９】　提供されたソフトウェアを実行する１つ以上のソフト実行器と、各ソフト実行器と通信経路を介して接続され、かつ各ソフト実行器から受けたソフトウェアの注文を管理する注文管理器とを備えたソフトウェア保護システムであって、
各前記ソフト実行器は、
固有の実行器ＩＤを格納する実行器ＩＤ格納手段と、
固有の実行器秘密情報を格納する第１の秘密情報格納手段と、
１つ以上のソフトウェアの実行権の注文情報を作成して蓄積保持する注文作成手段と、
前記注文作成手段で注文情報が作成される毎に変化し、所定のデータ構造または意味を有する変化値を生成して蓄積保持する変化値生成手段と、
前記注文情報および前記実行器秘密情報に依存した値を求め、この求めた値によって前記変化値を変換することにより、注文認証情報を生成して蓄積保持する注文認証情報生成手段とを含み、
前記実行器ＩＤ，前記注文情報および前記注文認証情報は、前記通信路を介して前記注文管理器に送付され、
前記注文管理器は、
各前記ソフト実行器に格納された全ての実行器秘密情報を格納する第２の秘密情報格納手段と、
前記ソフト実行器から受け取った実行器ＩＤに対応する実行器秘密情報を前記第２の秘密情報格納手段から獲得し、この獲得した実行器秘密情報とソフト実行器からの注文情報とに依存した値を求め、この値を用いてソフト実行器からの注文認証情報を逆変換する逆変換手段と、
前記逆変換手段の出力が前記変化値と同じデータ構造または意味を有する場合に、ソフト実行器および注文情報が正当であることを認証する実行器認証手段と、
前記実行器認証手段における認証結果が正当である場合にのみ、前記注文情報に依存した実行権生成パスワードを生成する実行権生成パスワード生成手段とを含み、
前記実行権生成パスワードは、前記通信路を介して前記ソフト実行器に送付され、
各前記ソフト実行器は、さらに前記注文作成手段に蓄積保持された注文情報と、前記注文認証情報生成手段に蓄積保持された注文認証情報とを用いて、前記注文管理器から受け取った実行権生成パスワードの正当性を検査する実行権生成パスワード検査手段と、
前記実行権生成パスワード検査手段による検査の結果、前記実行権生成パスワードの正当性が確認されたときに、前記注文作成手段に蓄積保持された注文情報に基づいて、注文されたソフトウェアの実行権を生成する実行権生成手段と、
前記実行権が存在するソフトウェアを、当該実行権に示される実行条件に従って実行するソフト実行手段とを含む、ソフトウェア保護システム。
【請求項１０】　前記注文認証情報生成手段は、前記注文作成手段によって作成された注文情報と、前記第１の秘密情報格納手段に格納された実行器秘密情報とを、出力が各入力ビットのすべてに関係するようなデータ圧縮関数に入力し、その出力結果と前記変化値との排他的論理和を注文認証情報として出力し、前記逆変換手段は、

ソフト実行器からの注文情報と、前記第２の秘密情報格納手段から獲得した実行器秘密情報とを、前記注文認証情報生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、その出力結果とソフト実行器からの注文認証情報との排他的論理和を演算することにより、当該注文認証情報を逆変換し、
前記実行権生成パスワード生成手段は、前記ソフト実行器から受け取った注文情報および前記注文識別情報を、前記注文認証情報生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、このデータ圧縮関数の出力結果を、前記実行権生成パスワードとして出力し、
前記実行権生成パスワード検査手段は、前記注文作成手段に蓄積保持された注文情報と、前記注文認証情報生成手段に蓄積保持された注文認証情報とを、前記注文認証情報生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、その出力結果が注文管理器から受け取った実行権生成パスワードと一致したとき、当該実行権生成パスワードが正当であると判断することを特徴とする、請求項９に記載のソフトウェア保護システム。

【請求項１１】　前記実行権生成パスワード生成手段は、ソフト実行器から受け取った注文情報に加えて、前記第２の秘密情報格納手段から獲得した実行器秘密情報に依存した実行権生成パスワードを生成し、
前記実行権生成パスワード検査手段は、前記注文作成手段に蓄積保持された注文情報と、前記第１の秘密情報格納手段に格納されている実行器秘密情報とを用いて、前記注文管理器から受け取った実行権生成パスワードの正当性を検査することを特徴とする、請求項７または９に記載のソフトウェア保護システム。

【請求項１２】　前記注文管理器は、公開鍵署名方式に用いられる秘密情報を格納する第３の秘密情報格納手段をさらに含み、
前記実行権生成パスワード生成手段は、前記第３の秘密情報格納手段に格納された秘密情報と、前記第２の秘密情報格納手段から獲得した実行器秘密情報と、前記ソフト実行器から受け取った注文情報および注文認証情報とを用いて、公開鍵署名方式によってデジタル署名された実行権生成パスワードを生成し、
前記ソフト実行器は、前記公開鍵署名方式に用いられる秘密情報に対応した公開情報を格納する公開情報格納手段をさらに含み、
前記実行権生成パスワード検査手段は、前記公開情報格納手段に格納された公開情報と、前記注文作成手段に蓄積保持された注文情報と、前記注文認証情報生成手段に蓄積保持された注文認証情報と、前記第１の秘密情報格納手段に格納された実行器秘密情報とを用いて、前記公開鍵署名方式に対応した署名確認方式によって、前記注文管理器から受け取った実行権生成パスワードの正当性を検査することを特徴とする、請求項７または９に記載のソフトウェア保護システム。

【請求項１３】　提供されたソフトウェアを実行する１つ以上のソフト実行器と、各ソフト実行器と通信経路を介して接続され、かつ各ソフト実行器から受けたソフトウェアの注文を管理する注文管理器とを備えたソフトウェア保護システムであって、
各前記ソフト実行器は、
固有の実行器ＩＤを格納する実行器ＩＤ格納手段と、
固有の実行器秘密情報を格納する第１の秘密情報格納手段と、
１つ以上のソフトウェアの実行権の注文情報を作成して蓄積保持する注文作成手段とを含み、
前記実行器ＩＤおよび前記注文情報は、前記通信路を介して前記注文管理器に送付され、
前記注文管理器は、
第１の実行権生成モジュールを格納する第１のモジュール格納手段と、
各前記ソフト実行器に格納された全ての実行器秘密情報を格納する第２の秘密情報格納手段と、
前記ソフト実行器からの注文情報と、前記第２の秘密情報格納手段から獲得した実行器秘密情報とに依存した値を計算する第１の計算手段と、
前記第１の計算手段の計算結果を用いて、前記第１の実行権生成モジュールを変換することにより、実行権生成パスワードを生成する実行権生成パスワード生成手段とを含み、
前記実行権生成パスワードは、前記通信路を介して前記ソフト実行器に送付され、
各ソフト実行器は、さらに第２の実行権生成モジュールを格納する第２のモジュール格納手段と、
前記注文作成手段に蓄積保持された注文情報と、前記第１の秘密情報格納手段に格納された実行器秘密情報とに依存した値を計算する第２の計算手段と、
前記第２の計算手段の計算結果を用いて、前記注文管理器からの実行権生成パスワードを逆変換することにより、第１の実行権生成モジュールを生成する実行権生成パスワード逆変換手段と、
前記実行権生成パスワード逆変換手段により生成された第１の実行権生成モジュールと、前記第２のモジュール格納手段に格納されている第２の実行権生成モジュールとを用いて、前記注文作成手段に蓄積保持された注文情報に基づくソフトウェアの実行権を生成する実行権生成手段と、
実行権生成後、第一の実行権生成モジュールを消去するモジュール消去手段と、
前記実行権が存在するソフトウェアを、当該実行権に示される実行条件に従って実行するソフト実行手段とを含む、ソフトウェア保護システム。

【請求項１４】　前記第１のモジュール格納手段に格納されている第１の実行権生成モジュールは、所定のデータ構造や意味をもっており、

前記実行権生成手段は、前記実行権生成パスワード逆変換手段の逆変換結果が前記第１の実行権生成モジュールと同じデータ構造や意味を持っている場合にのみ、第１の実行権生成モジュールと、第２の実行権生成モジュールとを用いて、前記注文作成手段に蓄積保持された注文情報に基づくソフトウェアの実行権を生成することを特徴とする、請求項１３に記載のソフトウェア保護システム。

【請求項１５】　前記注文管理器は、公開鍵署名方式に用いられる秘密情報を格納する第３の秘密情報格納手段をさらに含み、

前記実行権生成パスワード生成手段は、前記第１の計算手段の計算結果と、前記第３の秘密情報格納手段に格納された秘密情報とを用いて、前記第１の実行権生成モジュールを変換することにより、公開鍵署名方式によってデジタル署名された実行権生成パスワードを生成し、

前記ソフト実行器は、前記公開鍵署名方式に用いられる秘密情報に対応した公開情報を格納する公開情報格納手段をさらに含み、

前記実行権生成パスワード逆変換手段は、前記第２の計算手段の計算結果と、前記公開情報とを用い、前記公開鍵署名方式に対応した署名確認方式によって、前記注文管理器からの実行権生成パスワードを逆変換することを特徴とする、請求項１３に記載のソフトウェア保護システム。

【請求項１６】　前記ソフト実行器に提供されるソフトウェアは、ソフト固有情報を含んで暗号化されており、

前記実行権生成手段は、前記実行権生成パスワード検査手段が前記注文管理器からの実行権生成パスワードの正当性を確認したとき、前記注文作成手段に蓄積保持された注文情報に対応する暗号化ソフトウェアを復号して前記ソフト固有情報を獲得し、この獲得したソフト固有情報を前記実行器秘密情報で暗号化することによって、注文されたソフトウェアの実行権を生成し、

前記ソフト実行手段は、前記注文作成手段に蓄積保持された注文情報に対応する暗号化ソフトウェアを復号してソフトウェアとソフト固有情報とを獲得し、前記実行権を実行器秘密情報を用いて復号してソフト固有情報を獲得し、これら復号によって獲得したソフト固有情報が一致している場合にのみ、復号されたソフトウェアを実行することを特徴とする、請求項１～１５のいずれかに記載のソフトウェア保護システム。

【請求項１７】　前記注文作成手段は、作成した注文情報を不揮発的に蓄積保持し、前記実行権生成手段が対応するソフトウェアの実行権を生成した後に当該注文情報を消去することを特徴とする、請求項１～１５のいずれかに記載のソフトウェア保護システム。

【請求項１８】　前記ソフト実行器および前記注文管理器は、それぞれ相互間でやりとりされた情報の履歴を保持していることを特徴とする、請求項１～１５のいずれかに記載のソフトウェア保護システム。

【請求項１９】　前記ソフト実行器および前記注文管理器は、すべてのソフトウェアの組み合わせに対応するコードをテーブルとして保持しており、

前記ソフト実行器は、前記テーブルから得たコードを、前記注文情報として前記注文管理器に送付することを特徴とする、請求項１～１５のいずれかに記載のソフトウェア保護システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、ソフトウェア保護システムに関し、より特定的には、ソフトウェアを不活性な状態で配付しておき、電話などの通信路を用いてソフトウェアを活性化するための実行権を獲得するソフトウェア保護システムに関する。

【０００２】

【従来の技術】近年、種々のマルチメディア機器が開発され、ゲームや教育用のソフトウェアを始めとする多くの有償マルチメディアソフトウェアが販売されている。ところが、そのソフトウェアの保護は不完全であり、不正にコピーされたソフトウェアが数多く出回っているのが現状である。このような不正コピーを防ぐために特許法や著作権法等法律の規制があるが、同時にメカニズム面からのソフトウェア保護が強く要望されている。

【０００３】例えば、フロッピーディスク等の、ソフトウェアを格納する記録媒体のフォーマットを特殊なものにすることによって、ＯＳ（オペレーティング・システム）で提供されているコピー機能では複製ができないようにする方法がある。しかしながら、このような方法でもビットごとにコピーを行なうタイプのコピーツールを用いれば、多くの場合複製が可能である。また、正規のユーザにとっては、バックアップが作れないといった不都合も生じる。

【０００４】また、ソフトウェアを暗号化してコピー防止を行なう方法が提案されている。この方法では、ソフトウェアは暗号化されて不活性な状態でユーザに配付される。そして、ユーザの注文により、そのソフトウェアを特定の機器で活性化するための実行権（以下の従来例では、暗号化ファイルキー）が配付される。この実行権は、特定の機器に依存した情報なので、これを用いて他の機器で同じソフトウェアを活性化することはできない。この方法は、例えば特公平２－６０００７号公報に開示されている。その構成を図６に示す。なおこの図６は、特公平２－６０００７号公報の第１～第６図から説明上必要な部分を取り出して、１つの図にまとめ直したものである。

【０００５】図６において、このソフトウェア保護システムは、ソフトウェアを実行するソフト実行器６０１と、ソフト実行器６０１に対してソフトウェアを配付する注文管理器６０２とを備えている。

【０００６】ソフト実行器６０１は、暗号化ソフトウェア格納部６０３と、注文作成部６０４と、実行器ＩＤ格納部６０５と、実行器ＩＤに対応した固有の実行器暗号キーを格納する暗号キー格納部６０６と、注文管理器６０２から受け取った暗号化ファイルキーを格納する暗号化ファイルキー格納部６０７と、暗号化ファイルキーを実行器暗号キーで復号してファイルキーを獲得する暗号化ファイルキー復号部６０８と、ファイルキーを用いて暗号化ソフトウェアを復号し実行するソフト復号実行部６０９とを含む。このような構成のソフト実行器６０１は、注文作成部６０４での注文と、実行器ＩＤとを注文管理器６０２に伝えて、暗号化ソフトウェアを実行するための暗号化ファイルキーを要求する。

【０００７】注文管理器６０２は、すべてのソフトウェアのファイルキーを格納しているファイルキー格納部６１０と、すべてのソフト実行器の実行器暗号キーを格納している実行器暗号キー格納部６１１と、ファイルキーを指定の実行器暗号キーで暗号化して暗号化ファイルキーを生成する暗号化ファイルキー生成部６１２とを含む。このような構成の注文管理器６０２は、ソフト実行器６０１から指定されたソフトウェアのファイルキーをファイルキー格納部６１０から取り出し、また実行器暗号キー格納部６１１から実行器ＩＤに対応した暗号キーを取り出す。

【０００８】次に、図６に示す従来のソフトウェア保護システムの動作を説明する。暗号化ソフトウェアは、ソフトウェア固有のファイルキーで元のソフトウェアを暗号化したものである。この暗号化ソフトウェアは、複数個まとめられて、予め例えばＣＤ－ＲＯＭなどの記録媒体に格納され、ソフト実行器６０１に配付されている。配布された暗号化ソフトウェアは、暗号化ソフトウェア格納部６０３に格納されている。暗号化ソフトウェアは、これだけでは実行ができない不活性のソフトウェアである。実行を希望する場合には、注文作成部６０４で、注文のソフトウェアのＩＤを指定し、また、実行器ＩＤ格納部６０５に格納されているＩＤを注文管理器６０２に通知して注文を行なう。なお、この注文は、実用的には電話などを用いて行なわれる。

【０００９】注文管理器６０２において、ファイルキー格納部６１０は、ソフトＩＤを索引としてすべてのソフトウェアのファイルキーを格納している。また、実行器暗号キー格納部６１１は、実行器ＩＤを索引としてすべての実行器暗号キーを格納して管理している。そして、ソフト実行器６０１から注文を受け取った注文管理器６０２は、ファイルキー格納部６１０から注文のソフトウェアのファイルキーを獲得し、暗号化フィイルキー生成部６１２において、このファイルキーを、該当の実行器の暗号キーで暗号化して暗号化ファイルキーを作成する。そして、この暗号化ファイルキーをソフト実行器６０１に通知する。

【００１０】暗号化ファイルキーを受け取ったソフト実行器１００は、これを暗号化ファイルキー格納部１０７に格納しておく。そして、ソフトウェア実行時に、暗号化ファイルキー復号部１０８は、暗号化ファイルキー格納部１０７に格納された暗号化ファイルキーを、実行器暗号キー格納部１０６に格納された自分の暗号キーで復号して、ファイルキーを獲得する。ソフト復号実行部１０９は、暗号化ファイルキー復号部１０８で求められたファイルキーで暗号化ソフトウェアを復号し、ソフトウェアを実行する。なお、暗号化ファイルキーは、その実行器にのみ有効な情報なので、通信路や格納部から他人に獲得されても使用はできない。

【００１１】

【発明が解決しようとする課題】しかしながら、上記のような従来のソフトウェア保護システムでは、ソフトウェアの注文と、暗号化ファイルキーの受け取りとがすべて電話を介して行われるものとすると、以下に説明するように電話で伝える情報が多くなり、実用性に欠けたものになる。

【００１２】まず、ファイルキーと実行器暗号キーのビット数について述べる。ファイルキーは、元のソフトウェアを暗号化するための鍵である。また、実行器暗号キーは、このファイルキーを暗号化するための鍵である、ところで、ここでの暗号化には、秘密鍵ブロック暗号を用いるのが一般的である。秘密鍵ブロック暗号としては、米国で最も普及している暗号方式であるＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）、その後日本で開発されたＦＥＡＬ（Ｆａｓｔ　ｄａｔａ　Ｅｎｃｉｐｈｅｒｍｅｎｔ　Ａｌｇｏｒｉｔｈｍ）などが挙げられる。これらいずれの暗号化方式を採用する場合でも、安全性を確保するため、鍵のビット数は６４ビット程度必要であるというのが現状での認識である。従って、ファイルキーと実行器暗号キーとは、それぞれ６４ビット程度のデータとなる。なお、ＤＥＳについてはＦＩＰ　ＰＵＢ　４６，　ＮＢＳ　Ｊａｎ．，１９７７に、ＦＥＡＬについてはＡ．Ｓｈｉｍｉｚｕ　＆　Ｓ．Ｍｉｙａｇｕｃｈｉ：“Ｆａｓｔ　Ｄａｔａ　Ｅｎｃｉｐｈｅｒｍｅｎｔ　Ａｌｇｏｒｉｔｈｍ　ＦＥＡＬ”，　Ａｄｖａｎｃｅｓ　ｉｎ　Ｃｒｙｐｔｏｌｏｇｙ－ＥＵＲＯＣＲＹＰＴ’８７，　Ｓｐｒｉｎｇｅｒ書店に、それぞれ詳細に述べられている。

【００１３】次に、暗号化ファイルキーのビット数について述べる。暗号化ファイルキーは、ファイルキーを実行器暗号キーで暗号化したものである。上述したように、ファイルキーおよび実行器暗号キーは、６４ビット程度は必要であるため、この暗号化ファイルキーも６４ビット程度の値となる。６４ビットは、例えば１０進の数字で表すとすると、ほぼ２０桁くらいである。ところで、この暗号化ファイルキーは、注文管理器６０２を操作するオペレータから、ソフト実行器６０１を操作する

ユーザに対して、電話により口頭で伝えられる。さらに、ソフト実行器６０１のオペレータは、伝えられた暗号化ファイルキーを、ソフト実行器６０１に入力する必要がある。しかしながら、このように長い桁になると、言い間違え、聞き間違え、入力間違えの可能性が非常に大きくなり、実用的に問題が生じる。

【００１４】逆に、上記実用性を考慮して暗号化ファイルキーの桁数を小さくすると、これに伴いファイルキーや実行暗号キーのビット数が少なくなり、安全性が低下してしまう。

【００１５】また、上記従来例では、１つのソフトウェアの注文に対して１つの暗号化ファイルキーが対応する。従って、Ｎ個のソフトウェアの注文に対しては、伝える情報量はＮ倍となる。

【００１６】なお、上記従来例では、ソフトウェアに対する暗号化ファイルキーを一旦獲得した後は、そのソフトウェアを何度でも実行できる、いわば「実行権買い取り式」になっている。しかしながら、ソフトウェアの種類によっては、ソフトウェアの使用量に応じて料金を支払う形態の方がむしろ都合が良い場合がある。この形態では、たとえば、注文管理器からうけとった実行権を用いて、所定の回数だけの実行が可能となる。

【００１７】本発明の第１の目的は、安全性を劣化させずに（例えば、暗号の鍵のビット数を削減せずに）、ソフト実行器と注文管理器との間の情報量を削減することのできるソフトウェア保護システムを提供することである。

【００１８】本発明の第２の目的は、ソフト実行器と注文管理器との間の情報量が、注文するソフトの個数に依存しない（すなわち、Ｎ個のソフトを注文する場合の情報量が、１個ソフトを注文する場合の情報量と同じになる）ようなソフトウェア保護システムを提供することである。

【００１９】本発明の第３の目的は、回数制限等の条件付きの実行権に柔軟に対応するソフトウェア保護システムを提供することである。

【００２０】

【課題を解決するための手段】請求項１に係る発明は、提供されたソフトウェアを実行する１つ以上のソフト実行器と、各ソフト実行器と通信経路を介して接続され、かつ各ソフト実行器から受けたソフトウェアの注文を管理する注文管理器とを備えたソフトウェア保護システムであって、各ソフト実行器は、固有の実行器ＩＤを格納する実行器ＩＤ格納手段と、固有の実行器秘密情報を格納する第１の秘密情報格納手段と、１つ以上のソフトウェアの実行権の注文情報を作成して蓄積保持する注文作成手段とを含み、実行器ＩＤおよび注文情報は、通信路を介して注文管理器に送付され、注文管理器は、各ソフト実行器に格納された全ての実行器秘密情報を格納する第２の秘密情報格納手段と、ソフト実行器から受け取った実行器ＩＤに対応する実行器秘密情報を第２の秘密情報格納手段から獲得し、この獲得した実行器秘密情報およびソフト実行器から受け取った注文情報に依存した実行権生成パスワードを生成する実行権生成パスワード生成手段とを含み、実行権生成パスワードは、通信路を介してソフト実行器に送付され、各ソフト実行器は、さらに注文作成手段に蓄積保持された注文情報と、第１の秘密情報格納手段に格納された実行器秘密情報とを用いて、注文管理器から受け取った実行権生成パスワードの正当性を検査する実行権生成パスワード検査手段と、実行権生成パスワード検査手段による検査の結果、実行権生成パスワードの正当性が確認されたときに、注文作成手段に蓄積保持された注文情報に基づいて、注文されたソフトウェアの実行権を生成する実行権生成手段と、実行権が存在するソフトウェアを、当該実行権に示される実行条件に従って実行するソフト実行手段とを含んでいる。

【００２１】請求項２に係る発明は、請求項１の発明において、実行権生成パスワード生成手段は、ソフト実行器から受け取った注文情報と、第２の秘密情報格納手段から獲得した実行器秘密情報とを、出力が入力ビットのすべてに関係するようなデータ圧縮関数に入力し、このデータ圧縮関数の出力結果を、実行権生成パスワードとして出力し、実行権生成パスワード検査手段は、注文作成手段に蓄積保持された注文情報と、第１の秘密情報格納手段に格納された実行器秘密情報とを、実行権生成パスワード生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、その出力結果が注文管理器から受け取った実行権生成パスワードと一致したとき、当該実行権生成パスワードが正当であると判断することを特徴とする。

【００２２】請求項３に係る発明は、請求項１の発明において、注文管理器は、公開鍵署名方式に用いられる秘密情報を格納する第３の秘密情報格納手段をさらに含み、実行権生成パスワード生成手段は、第３の秘密情報格納手段に格納された秘密情報と、第２の秘密情報格納手段から獲得した実行器秘密情報と、ソフト実行器から受け取った注文情報と用いて、公開鍵署名方式によってデジタル署名された実行権生成パスワードを生成し、ソフト実行器は、公開鍵署名方式に用いられる秘密情報に対応した公開情報を格納する公開情報格納手段をさらに含み、実行権生成パスワード検査手段は、公開情報格納手段に格納された公開情報と、注文作成手段に蓄積保持された注文情報と、第１の秘密情報格納手段に格納された実行器秘密情報とを用いて、公開鍵署名方式に対応した署名確認方式によって、注文管理器から受け取った実行権生成パスワードの正当性を検査することを特徴とする。

【００２３】請求項４に係る発明は、提供されたソフトウェアを実行する１つ以上のソフト実行器と、各ソフト

実行器と通信経路を介して接続され、かつ各ソフト実行器から受けたソフトウェアの注文を管理する注文管理器とを備えたソフトウェア保護システムであって、各ソフト実行器は、固有の実行器ＩＤを格納する実行器ＩＤ格納手段と、固有の実行器秘密情報を格納する第１の秘密情報格納手段と、１つ以上のソフトウェアの実行権の注文情報を作成して蓄積保持する注文作成手段と、注文作成手段で注文情報が作成される毎に変化する変化値を生成して蓄積保持する変化値生成手段とを含み、実行器ＩＤ，注文情報および変化値は、通信路を介して注文管理器に送付され、注文管理器は、各ソフト実行器に格納された全ての実行器秘密情報を格納する第２の秘密情報格納手段と、ソフト実行器から受け取った実行器ＩＤに対応する実行器秘密情報を第２の秘密情報格納手段から獲得し、この獲得した実行器秘密情報，ソフト実行器から受け取った注文情報および変化値に依存した実行権生成パスワードを生成する実行権生成パスワード生成手段とを含み、実行権生成パスワードは、通信路を介してソフト実行器に送付され、各ソフト実行器は、さらに注文作成手段に蓄積保持された注文情報と、変化値生成手段に蓄積保持された変化値と、第１の秘密情報格納手段に格納された実行器秘密情報とを用いて、注文管理器から受け取った実行権生成パスワードの正当性を検査する実行権生成パスワード検査手段と、実行権生成パスワード検査手段による検査の結果、実行権生成パスワードの正当性が確認されたときに、注文作成手段に蓄積保持された注文情報に基づいて、注文されたソフトウェアの実行権を生成する実行権生成手段と、実行権が存在するソフトウェアを、当該実行権に示される実行条件に従って実行するソフト実行手段とを含んでいる。

【００２４】請求項５に係る発明は、請求項４の発明において、実行権生成パスワード生成手段は、ソフト実行器から受け取った注文情報および変化値と、第２の秘密情報格納手段から獲得した実行器秘密情報とを、出力が入力ビットのすべてに関係するようなデータ圧縮関数に入力し、このデータ圧縮関数の出力結果を、実行権生成パスワードとして出力し、実行権生成パスワード検査手段は、注文作成手段に蓄積保持された注文情報と、変化値生成手段に蓄積保持された変化値と、第１の秘密情報格納手段に格納された実行器秘密情報とを、実行権生成パスワード生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、その出力結果が注文管理器から受け取った実行権生成パスワードと一致したとき、当該実行権生成パスワードが正当であると判断することを特徴とする。

【００２５】請求項６に係る発明は、提供されたソフトウェアを実行する１つ以上のソフト実行器と、各ソフト実行器と通信経路を介して接続され、かつ各ソフト実行器から受けたソフトウェアの注文を管理する注文管理器とを備えたソフトウェア保護システムであって、各ソフト実行器は、固有の実行器ＩＤを格納する実行器ＩＤ格納手段と、固有の実行器秘密情報を格納する第１の秘密情報格納手段と、１つ以上のソフトウェアの実行権の注文情報を作成して蓄積保持する注文作成手段と、注文作成手段で注文情報が作成される毎にタイムスタンプを生成して蓄積保持する第１のタイムスタンプ生成手段とを含み、実行器ＩＤおよび注文情報は、通信路を介して注文管理器に送付され、注文管理器は、ソフト実行器から実行器ＩＤおよび注文情報を受け取ると、タイムスタンプを生成する第２のタイムスタンプ生成手段と、各ソフト実行器に格納された全ての実行器秘密情報を格納する第２の秘密情報格納手段と、ソフト実行器から受け取った実行器ＩＤに対応する実行器秘密情報を第２の秘密情報格納手段から獲得し、この獲得した実行器秘密情報と、ソフト実行器から受け取った注文情報と、第２のタイムスタンプ生成手段で生成されたタイムスタンプとに依存した実行権生成パスワードを生成する実行権生成パスワード生成手段とを含み、実行権生成パスワードは、通信路を介してソフト実行器に送付され、各ソフト実行器は、さらに注文作成手段に蓄積保持された注文情報と、第１のタイムスタンプ生成手段に蓄積保持されたタイムスタンプと、第１の秘密情報格納手段に格納された実行器秘密情報とを用いて、注文管理器から受け取った実行権生成パスワードの正当性を検査する実行権生成パスワード検査手段と、実行権生成パスワード検査手段による検査の結果、実行権生成パスワードの正当性が確認されたときに、注文作成手段に蓄積保持された注文情報に基づいて、注文されたソフトウェアの実行権を生成する実行権生成手段と、実行権が存在するソフトウェアを、当該実行権に示される実行条件に従って実行するソフト実行手段とを含んでいる。

【００２６】請求項７に係る発明は、提供されたソフトウェアを実行する１つ以上のソフト実行器と、各ソフト実行器と通信経路を介して接続され、かつ各ソフト実行器から受けたソフトウェアの注文を管理する注文管理器とを備えたソフトウェア保護システムであって、各ソフト実行器は、固有の実行器ＩＤを格納する実行器ＩＤ格納手段と、固有の実行器秘密情報を格納する第１の秘密情報格納手段と、１つ以上のソフトウェアの実行権の注文情報を作成して蓄積保持する注文作成手段と、注文情報と実行器秘密情報に依存した注文認証情報を生成して蓄積保持する注文認証情報生成手段とを含み、実行器ＩＤ，注文情報および注文認証情報は、通信路を介して注文管理器に送付され、注文管理器は、各ソフト実行器に格納された全ての実行器秘密情報を格納する第２の秘密情報格納手段と、ソフト実行器から受け取った実行器ＩＤに対応する実行器秘密情報を第２の秘密情報格納手段から獲得し、この獲得した実行器秘密情報，ソフト実行器から受け取った注文情報および注文認証情報を用いて、ソフト実行器および注文情報の認証を行い、この認

証結果が正当である場合に、当該注文認証情報を注文を識別する注文識別情報として扱う実行器認証手段と、実行器認証手段における認証結果が正当である場合にのみ、注文情報および注文識別情報に依存した実行権生成パスワードを生成する実行権生成パスワード生成手段とを含み、実行権生成パスワードは、注文識別情報と共に、通信路を介してソフト実行器に送付され、各ソフト実行器は、さらに注文作成手段に蓄積保持された注文情報と、注文認証情報生成手段に蓄積保持された注文認証情報とを用いて、注文管理器から受け取った実行権生成パスワードの正当性を検査する実行権生成パスワード検査手段と、実行権生成パスワード検査手段による検査の結果、実行権生成パスワードの正当性が確認されたときに、注文作成手段に蓄積保持された注文情報に基づいて、注文されたソフトウェアの実行権を生成する実行権生成手段と、実行権が存在するソフトウェアを、当該実行権に示される実行条件に従って実行するソフト実行手段とを含んでいる。

【００２７】請求項８に係る発明は、請求項７の発明において、注文認証情報生成手段は、注文作成手段によって作成された注文情報と、第１の秘密情報格納手段に格納された実行器秘密情報とを、出力が入力ビットのすべてに関係するようなデータ圧縮関数に入力し、このデータ圧縮関数の出力結果を、注文認証情報として出力し、実行器認証手段は、第２の秘密情報格納手段から獲得した実行器秘密情報と、ソフト実行器から受け取った注文情報とを、注文認証情報生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、このデータ圧縮関数の出力結果がソフト実行器から受け取った注文認証情報と一致する場合に、注文を行ったソフト実行器および注文情報が正当であることを認証し、実行権生成パスワード生成手段は、ソフト実行器から受け取った注文情報および注文識別情報を、注文認証情報生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、このデータ圧縮関数の出力結果を、実行権生成パスワードとして出力し、実行権生成パスワード検査手段は、注文作成手段に蓄積保持された注文情報と、注文認証情報生成手段に蓄積保持された注文認証情報とを、注文認証情報生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、その出力結果が注文管理器から受け取った実行権生成パスワードと一致したとき、当該実行権生成パスワードが正当であると判断することを特徴とする。

【００２８】請求項９に係る発明は、提供されたソフトウェアを実行する１つ以上のソフト実行器と、各ソフト実行器と通信経路を介して接続され、かつ各ソフト実行器から受けたソフトウェアの注文を管理する注文管理器とを備えたソフトウェア保護システムであって、各ソフト実行器は、固有の実行器ＩＤを格納する実行器ＩＤ格納手段と、固有の実行器秘密情報を格納する第１の秘密情報格納手段と、１つ以上のソフトウェアの実行権の注文情報を作成して蓄積保持する注文作成手段と、注文作成手段で注文情報が作成される毎に変化し、所定のデータ構造または意味を有する変化値を生成して蓄積保持する変化値生成手段と、注文情報および実行器秘密情報に依存した値を求め、この求めた値によって変化値を変換することにより、注文認証情報を生成して蓄積保持する注文認証情報生成手段とを含み、実行器ＩＤ，注文情報および注文認証情報は、通信路を介して注文管理器に送付され、注文管理器は、各ソフト実行器に格納された全ての実行器秘密情報を格納する第２の秘密情報格納手段と、ソフト実行器から受け取った実行器ＩＤに対応する実行器秘密情報を第２の秘密情報格納手段から獲得し、この獲得した実行器秘密情報とソフト実行器からの注文情報とに依存した値を求め、この値を用いてソフト実行器からの注文認証情報を逆変換する逆変換手段と、逆変換手段の出力が変化値と同じデータ構造または意味を有する場合に、ソフト実行器および注文情報が正当であることを認証する実行器認証手段と、実行器認証手段における認証結果が正当である場合にのみ、注文情報に依存した実行権生成パスワードを生成する実行権生成パスワード生成手段とを含み、実行権生成パスワードは、通信路を介してソフト実行器に送付され、各ソフト実行器は、さらに注文作成手段に蓄積保持された注文情報と、注文認証情報生成手段に蓄積保持された注文認証情報とを用いて、注文管理器から受け取った実行権生成パスワードの正当性を検査する実行権生成パスワード検査手段と、実行権生成パスワード検査手段による検査の結果、実行権生成パスワードの正当性が確認されたときに、注文作成手段に蓄積保持された注文情報に基づいて、注文されたソフトウェアの実行権を生成する実行権生成手段と、実行権が存在するソフトウェアを、当該実行権に示される実行条件に従って実行するソフト実行手段とを含んでいる。

【００２９】請求項１０に係る発明は、請求項９の発明において、注文認証情報生成手段は、注文作成手段によって作成された注文情報と、第１の秘密情報格納手段に格納された実行器秘密情報とを、出力が各入力ビットのすべてに関係するようなデータ圧縮関数に入力し、その出力結果と変化値との排他的論理和を注文認証情報として出力し、逆変換手段は、ソフト実行器からの注文情報と、第２の秘密情報格納手段から獲得した実行器秘密情報とを、注文認証情報生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、その出力結果とソフト実行器からの注文認証情報との排他的論理和を演算することにより、当該注文認証情報を逆変換し、実行権生成パスワード生成手段は、ソフト実行器から受け取った注文情報および注文識別情報を、注文認証情報生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、このデータ圧縮関数の出力結果を、実行権生成

パスワードとして出力し、実行権生成パスワード検査手段は、注文作成手段に蓄積保持された注文情報と、注文認証情報生成手段に蓄積保持された注文認証情報とを、注文認証情報生成手段で用いているデータ圧縮関数と同じデータ圧縮関数に入力し、その出力結果が注文管理器から受け取った実行権生成パスワードと一致したとき、当該実行権生成パスワードが正当であると判断することを特徴とする。

【００３０】請求項１１に係る発明は、請求項７または９の発明において、実行権生成パスワード生成手段は、ソフト実行器から受け取った注文情報に加えて、第２の秘密情報格納手段から獲得した実行器秘密情報に依存した実行権生成パスワードを生成し、実行権生成パスワード検査手段は、注文作成手段に蓄積保持された注文情報と、第１の秘密情報格納手段に格納されている実行器秘密情報とを用いて、注文管理器から受け取った実行権生成パスワードの正当性を検査することを特徴とする。

【００３１】請求項１２に係る発明は、請求項７または９の発明において、注文管理器は、公開鍵署名方式に用いられる秘密情報を格納する第３の秘密情報格納手段をさらに含み、実行権生成パスワード生成手段は、第３の秘密情報格納手段に格納された秘密情報と、第２の秘密情報格納手段から獲得した実行器秘密情報と、ソフト実行器から受け取った注文情報および注文認証情報とを用いて、公開鍵署名方式によってデジタル署名された実行権生成パスワードを生成し、ソフト実行器は、公開鍵署名方式に用いられる秘密情報に対応した公開情報を格納する公開情報格納手段をさらに含み、実行権生成パスワード検査手段は、公開情報格納手段に格納された公開情報と、注文作成手段に蓄積保持された注文情報と、注文認証情報生成手段に蓄積保持された注文認証情報と、第１の秘密情報格納手段に格納された実行器秘密情報とを用いて、公開鍵署名方式に対応した署名確認方式によって、注文管理器から受け取った実行権生成パスワードの正当性を検査することを特徴とする。

【００３２】請求項１３に係る発明は、提供されたソフトウェアを実行する１つ以上のソフト実行器と、各ソフト実行器と通信経路を介して接続され、かつ各ソフト実行器から受けたソフトウェアの注文を管理する注文管理器とを備えたソフトウェア保護システムであって、各ソフト実行器は、固有の実行器ＩＤを格納する実行器ＩＤ格納手段と、固有の実行器秘密情報を格納する第１の秘密情報格納手段と、１つ以上のソフトウェアの実行権の注文情報を作成して蓄積保持する注文作成手段とを含み、実行器ＩＤおよび注文情報は、通信路を介して注文管理器に送付され、注文管理器は、第１の実行権生成モジュールを格納する第１のモジュール格納手段と、各ソフト実行器に格納された全ての実行器秘密情報を格納する第２の秘密情報格納手段と、ソフト実行器からの注文情報と、第２の秘密情報格納手段から獲得した実行器秘密情報とに依存した値を計算する第１の計算手段と、第１の計算手段の計算結果を用いて、第１の実行権生成モジュールを変換することにより、実行権生成パスワードを生成する実行権生成パスワード生成手段とを含み、実行権生成パスワードは、通信路を介してソフト実行器に送付され、各ソフト実行器は、さらに第２の実行権生成モジュールを格納する第２のモジュール格納手段と、注文作成手段に蓄積保持された注文情報と、第１の秘密情報格納手段に格納された実行器秘密情報とに依存した値を計算する第２の計算手段と、第２の計算手段の計算結果を用いて、注文管理器からの実行権生成パスワードを逆変換することにより、第１の実行権生成モジュールを生成する実行権生成パスワード逆変換手段と、実行権生成パスワード逆変換手段により生成された第１の実行権生成モジュールと、第２のモジュール格納手段に格納されている第２の実行権生成モジュールとを用いて、注文作成手段に蓄積保持された注文情報に基づくソフトウェアの実行権を生成する実行権生成手段と、実行権生成後、第一の実行権生成モジュールを消去するモジュール消去手段と、実行権が存在するソフトウェアを、当該実行権に示される実行条件に従って実行するソフト実行手段とを含んでいる。

【００３３】請求項１４に係る発明は、請求項１３の発明において、第１のモジュール格納手段に格納されている第１の実行権生成モジュールは、所定のデータ構造や意味をもっており、実行権生成手段は、実行権生成パスワード逆変換手段の逆変換結果が第１の実行権生成モジュールと同じデータ構造や意味を持っている場合にのみ、第１の実行権生成モジュールと、第２の実行権生成モジュールとを用いて、注文作成手段に蓄積保持された注文情報に基づくソフトウェアの実行権を生成することを特徴とする。

【００３４】請求項１５に係る発明は、請求項１３の発明において、注文管理器は、公開鍵署名方式に用いられる秘密情報を格納する第３の秘密情報格納手段をさらに含み、実行権生成パスワード生成手段は、第１の計算手段の計算結果と、第３の秘密情報格納手段に格納された秘密情報とを用いて、第１の実行権生成モジュールを変換することにより、公開鍵署名方式によってデジタル署名された実行権生成パスワードを生成し、ソフト実行器は、公開鍵署名方式に用いられる秘密情報に対応した公開情報を格納する公開情報格納手段をさらに含み、実行権生成パスワード逆変換手段は、第２の計算手段の計算結果と、公開情報とを用い、公開鍵署名方式に対応した署名確認方式によって、注文管理器からの実行権生成パスワードを逆変換することを特徴とする。

【００３５】請求項１６に係る発明は、請求項１～１５のいずれかに記載の発明において、ソフト実行器に提供されるソフトウェアは、ソフト固有情報を含んで暗号化されており、実行権生成手段は、実行権生成パスワード

検査手段が注文管理器からの実行権生成パスワードの正当性を確認したとき、注文作成手段に蓄積保持された注文情報に対応する暗号化ソフトウェアを復号してソフト固有情報を獲得し、この獲得したソフト固有情報を実行器秘密情報で暗号化することによって、注文されたソフトウェアの実行権を生成し、ソフト実行手段は、注文作成手段に蓄積保持された注文情報に対応する暗号化ソフトウェアを復号してソフトウェアとソフト固有情報とを獲得し、実行権を実行器秘密情報を用いて復号してソフト固有情報を獲得し、これら復号によって獲得したソフト固有情報が一致している場合にのみ、復号されたソフトウェアを実行することを特徴とする。

【００３６】請求項１７に係る発明は、請求項１～１５のいずれかに記載の発明において、注文作成手段は、作成した注文情報を不揮発的に蓄積保持し、実行権生成手段が対応するソフトウェアの実行権を生成した後に当該注文情報を消去することを特徴とする。

【００３７】請求項１８に係る発明は、請求項１～１５のいずれかに記載の発明において、ソフト実行器および注文管理器は、それぞれ相互間でやりとりされた情報の履歴を保持していることを特徴とする。

【００３８】請求項１９に係る発明は、請求項１～１５のいずれかに記載の発明において、ソフト実行器および注文管理器は、すべてのソフトウェアの組み合わせに対応するコードをテーブルとして保持しており、ソフト実行器は、テーブルから得たコードを、注文情報として注文管理器に送付することを特徴とする。

【００３９】

【作用】請求項１に係る発明では、ソフト実行器は、実行器ＩＤおよび注文情報を生成し、これらを注文管理器に送付することにより、ソフトウェアの注文を行なう。注文管理器は、受け取った注文情報と、実行ＩＤに対応する実行器秘密情報とに依存した情報である実行権生成パスワードを生成し、ソフト実行器に送付する。ソフト実行器は、この実行権生成パスワードが、注文管理器に先に送付した注文情報や、自分自身の実行器秘密情報と整合している否かを判断し、整合している場合は、注文情報に対応したソフトウェアの実行権を生成し、当該ソフトウェアを実行する。このように、注文管理器からソフト実行器には、実行権生成パスワード、すなわちソフト実行器が注文情報に対応したソフト実行権を生成するための許可を与える情報だけが送付されるため、実行権そのものを送付する場合に比べて、桁数を削減できる。また、ソフト実行器が複数のソフトウェアの注文を１回に行なっても、その情報量は１つのソフトウェアを注文した場合の情報量と同じになる。

【００４０】請求項２に係る発明では、注文管理器は、ソフト実行器から受け取った注文情報と、実行器ＩＤに対応する実行器秘密情報とを、所定のデータ圧縮関数（例えば、ハッシュ関数）に入力し、このデータ圧縮関数の出力結果を、実行権生成パスワードとして出力する。一方、ソフト実行器は、内部に蓄積保持された注文情報と、自分自身の実行器秘密情報とを、上記と同様のデータ圧縮関数に入力し、その出力結果が注文管理器から受け取った実行権生成パスワードと一致したとき、当該実行権生成パスワードが正当であると判断する。このように、データ圧縮関数を用いて実行権生成パスワードが生成されるので、その桁数をより一層削減できる。

【００４１】請求項３に係る発明では、注文管理器は、公開鍵署名方式に用いられる秘密情報を保持し、この秘密情報と、実行器ＩＤに対応する実行器秘密情報と、ソフト実行器から受け取った注文情報と用いて、公開鍵署名方式によってデジタル署名された実行権生成パスワードを生成する。一方、ソフト実行器は、公開鍵署名方式に用いられる秘密情報に対応した公開情報を保持し、この公開情報と、注文情報と、自分自身の実行器秘密情報とを用いて、公開鍵署名方式に対応した署名確認方式によって、注文管理器から受け取った実行権生成パスワードの正当性を検査する。このように、ソフト実行器には、デジタル署名された実行権生成パスワードが送付されるので、ソフト実行器側で実行権生成パスワードを偽造することがほとんど不可能となり、極めて安全性の高いソフトウェア保護システムが実現できる。

【００４２】請求項４に係る発明では、注文情報を作成する毎に変化する変化値が注文情報と共に、ソフト実行器から注文管理器に送付される。そして、注文管理器は、実行器秘密情報，注文情報および変化値に依存した実行権生成パスワードを生成し、注文管理器に送付する。ソフト実行器は、注文情報，変化値および実行器秘密情報を用いて、実行権生成パスワードの正当性を検査する。従って、注文管理器からの実行権生成パスワードは、対応する変化値を保持するソフト実行器でのみ有効となる。そのため、異なる時期に同じ注文を作成し、以前の実行権生成パスワードを入力しても、後の注文時に生成される変化値は、以前の注文時に生成される変化値とは異なっているため、入力したパスワードが有効にはならない。

【００４３】請求項５に係る発明では、注文管理器は、注文情報，変化値および実行器秘密情報を、ハッシュ関数等のデータ圧縮関数に入力し、このデータ圧縮関数の出力結果を、実行権生成パスワードとして出力する。一方、ソフト実行器は、内部に保持している注文情報，変化値および実行器秘密情報を、上記と同様のデータ圧縮関数に入力し、その出力結果が注文管理器から受け取った実行権生成パスワードと一致したとき、当該実行権生成パスワードが正当であると判断する。このように、データ圧縮関数を用いて実行権生成パスワードが生成されるので、その桁数をより一層削減できる。

【００４４】請求項６に係る発明では、請求項４における変化値の代わりにタイムスタンプを用いている。この

タイムスタンプは、ソフト実行器と注文管理器とに共通に保持されているため、請求項４のようにソフト実行器から注文管理器に変化値を送付する必要がなくなる。

【００４５】請求項７に係る発明では、注文情報および実行器秘密情報に依存した注文認証情報を導入することにより、注文管理器側で実行権生成パスワードの発行に先だって、注文情報とソフト実行器の認証を行うことができる。そして、注文管理器は、認証結果がＯＫの場合には、上記注文認証情報を注文を識別する注文識別情報として扱い、これら注文情報および注文識別情報に依存した実行権生成パスワードを生成してソフト実行器に送付する。ソフト実行器は、内部に保持している注文情報および注文認証情報を用いて、注文管理器から受け取った実行権生成パスワードの正当性を検査し、この検査結果がＯＫのときに、ソフトウェアの実行権を生成し、対応するソフトウェアを実行する。

【００４６】請求項８に係る発明では、ソフト実行器は、注文情報および実行器秘密情報を、ハッシュ関数等のデータ圧縮関数に入力し、このデータ圧縮関数の出力結果を、注文認証情報として得ている。また、注文管理器は、実行器秘密情報と、ソフト実行器から受け取った注文情報とを、上記と同様のデータ圧縮関数に入力し、その出力結果がソフト実行器から受け取った注文認証情報と一致する場合に、ソフト実行器および注文情報が正当であることを認証する。さらに、注文管理器は、注文情報および注文識別情報を、上記と同様のデータ圧縮関数に入力し、このデータ圧縮関数の出力結果を、実行権生成パスワードとして出力し、ソフト実行器に送付する。一方、ソフト実行器は、注文情報および注文認証情報を、上記と同様のデータ圧縮関数に入力し、その出力結果が注文管理器からの実行権生成パスワードと一致したとき、当該実行権生成パスワードが正当であると判断する。

【００４７】請求項９に係る発明では、ソフト実行器は、注文情報の作成毎に変化しかつ所定のデータ構造または意味を有する変化値を、注文情報および実行器秘密情報に依存した値によって変換することにより、注文認証情報を生成する。この注文認証情報は、実行器ＩＤおよび注文情報と共に、注文管理器に送付される。注文管理器は、実行器ＩＤに対応する実行器秘密情報と、ソフト実行器からの注文情報とに依存した値を求め、この値を用いてソフト実行器からの注文認証情報を逆変換し、この逆変換結果が上記変化値と同じデータ構造または意味を有する場合に、ソフト実行器および注文情報が正当であることを認証する。そして、注文管理器は、この認証結果が正当である場合にのみ、注文情報に依存した実行権生成パスワードを生成してソフト実行器に送付する。ソフト実行器は、内部に保持している注文情報および注文認証情報を用いて、注文管理器から受け取った実行権生成パスワードの正当性を検査し、実行権生成パスワードの正当性が確認されたときに、注文されたソフトウェアの実行権を生成する。このような構成により、ソフト実行器と注文管理器間でやりとりされる情報量を増やすことなく、回数制限機能およびユーザ認証機能を実現できる。

【００４８】請求項１０に係る発明では、ソフト実行器は、注文情報および実行器秘密情報を、ハッシュ関数等のデータ圧縮関数に入力し、その出力結果と変化値との排他的論理和を注文認証情報として得ている。注文管理器は、ソフト実行器からの注文情報と、実行器ＩＤに対応する実行器秘密情報とを、上記と同様のデータ圧縮関数に入力し、その出力結果とソフト実行器からの注文認証情報との排他的論理和を演算することにより、当該注文認証情報を逆変換している。また、注文管理器は、ソフト実行器からの注文情報および注文識別情報を、上記と同様のデータ圧縮関数に入力し、このデータ圧縮関数の出力結果を、実行権生成パスワードとして出力するようにしている。ソフト実行器は、内部に保持している注文情報および注文認証情報を、上記と同様のデータ圧縮関数に入力し、その出力結果が注文管理器から受け取った実行権生成パスワードと一致したとき、当該実行権生成パスワードが正当であると判断する。

【００４９】請求項１１に係る発明では、注文管理器は、ソフト実行器から受け取った注文情報と、実行器ＩＤに対応する実行器秘密情報とに依存した実行権生成パスワードを生成する。一方、ソフト実行器は、内部に保持している注文情報および実行器秘密情報を用いて、注文管理器から受け取った実行権生成パスワードの正当性を検査する。

【００５０】請求項１２に係る発明では、注文管理器は、公開鍵署名方式に用いられる秘密情報と、実行器ＩＤに対応する実行器秘密情報と、ソフト実行器から受け取った注文情報および注文認証情報とを用いて、公開鍵署名方式によってデジタル署名された実行権生成パスワードを生成し、ソフト実行器に送付する。ソフト実行器は、公開鍵署名方式に用いられる秘密情報に対応した公開情報と、内部に保持している注文情報，注文認証情報および実行器秘密情報とを用い、公開鍵署名方式に対応した署名確認方式によって、注文管理器から受け取った実行権生成パスワードの正当性を検査する。このように、ソフト実行器には、デジタル署名された実行権生成パスワードが送付されるので、ソフト実行器側で実行権生成パスワードを偽造することがほとんど不可能となり、極めて安全性の高いソフトウェア保護システムが実現できる。

【００５１】請求項１３に係る発明では、ソフト実行器側に格納された第２の実行権生成モジュールだけでは、実行権の生成はできない。注文管理器は、この第２の実行権生成モジュールを活性化させるための第１の実行権生成モジュールを、ソフト実行器からの注文情報と実行

器秘密情報に依存した形に変換して実行権生成パスワードとして送付する。ソフト実行器側では、正しい注文情報と実行器である場合、この実行権生成パスワードを用いて、内部に保持している第２の実行権生成モジュールを活性化させることができる。この場合、ソフト実行器が不正に実行権を生成しようとしても、情報量的に第２の実行権生成モジュールにそのための情報が不足しているため不正はできない。そのため、より一層安全なソフトウェア保護システムが実現できる。

【００５２】請求項１４に係る発明では、注文管理器に格納されている第１の実行権生成モジュールは、所定のデータ構造や意味をもっており、ソフト実行器は、実行権生成パスワードの逆変換結果が第１の実行権生成モジュールと同じデータ構造や意味を持っている場合にのみ、第１の実行権生成モジュールと、第２の実行権生成モジュールとを用いて、ソフトウェアの実行権を生成する。

【００５３】請求項１５に係る発明では、注文管理器は、公開鍵署名方式に用いられる秘密情報と、注文情報および実行器秘密情報に依存した値である第１の計算手段の計算結果とを用いて、第１の実行権生成モジュールを変換することにより、公開鍵署名方式によってデジタル署名された実行権生成パスワードを生成する。一方、ソフト実行器は、公開鍵署名方式に用いられる秘密情報に対応した公開情報と、注文情報および実行器秘密情報に依存した値である第２の計算手段の計算結果とを用い、公開鍵署名方式に対応した署名確認方式によって、注文管理器からの実行権生成パスワードを逆変換する。

【００５４】請求項１６に係る発明では、ソフト実行器に提供されるソフトウェアは、ソフト固有情報を含んで暗号化されている。そして、ソフト実行器は、注文管理器からの実行権生成パスワードの正当性を確認したとき、内部に保持している注文情報に対応する暗号化ソフトウェアを復号してソフト固有情報を獲得し、この獲得したソフト固有情報を実行器秘密情報で暗号化することによって、注文されたソフトウェアの実行権を生成する。また、ソフト実行器は、内部に保持している注文情報に対応する暗号化ソフトウェアを復号してソフトウェアとソフト固有情報とを獲得し、実行権を実行器秘密情報を用いて復号してソフト固有情報を獲得し、これら復号によって獲得したソフト固有情報が一致している場合にのみ、復号されたソフトウェアを実行する。

【００５５】請求項１７に係る発明では、ソフト実行器は、作成した注文情報を不揮発的に蓄積保持し、対応するソフトウェアの実行権を生成した後に当該注文情報を消去する。これによって、とりあえず注文だけを連続して送付し、後に返送されてくる実行権生成パスワードに基づいて、ソフトウェアの実行を制御することができる。

【００５６】請求項１８に係る発明では、ソフト実行器および注文管理器は、それぞれ相互間でやりとりされた情報の履歴を保持している。これによって、後に生じるトラブル等に柔軟に対処できる。

【００５７】請求項１９に係る発明では、ソフト実行器および注文管理器は、すべてのソフトウェアの組み合わせに対応するコードをテーブルとして保持しており、ソフト実行器は、テーブルから得たコードを、注文情報として注文管理器に送付するようにしている。これによって、注文情報のデータ量をより一層削減できる。

【００５８】

【実施例】

（１）第１の実施例

図１は、本発明の第１の実施例に係るソフトウェア保護システムの構成を示すブロック図である。図１において、本実施例のソフトウェア保護システムは、ソフトウェアを実行するソフト実行器１０１と、ソフト実行器１０１に対してソフトウェアを配付する注文管理器１０２とを備えている。

【００５９】ソフト実行器１０１は、暗号化ソフトウェア格納部３と、注文作成部４と、実行器ＩＤ格納部５と、実行器ＩＤに対応した実行器暗号キー（実行器秘密情報の一例）を格納する実行器暗号キー格納部６と、注文管理器１０２から受け取った実行権生成パスワードの正当性を検査する実行権生成パスワード検査部７と、注文情報に基づいて実行器暗号キーを使用して実行権を生成する実行権生成部８と、生成した実行権を格納する実行権格納部９と、ソフトウェア実行時に対応する実行権が有効である場合に上記暗号化ソフトウェアを復号して実行するソフト復号実行部１０とを含む。このような構成のソフト実行器１０１において、注文作成部４で作成された注文情報と、実行器ＩＤとは、注文管理器１０２に伝えられ、暗号化ソフトウェアを実行するための実行権生成パスワードが要求される。

【００６０】一方、注文管理器１０２は、すべてのソフト実行器の実行器暗号キーを格納している実行器暗号キー格納部１１と、注文情報および該当のソフト実行器の実行器暗号鍵に依存した実行権生成パスワードを生成する実行権生成パスワード生成部１２とを含む。

【００６１】次に、図１に示す第１の実施例のソフトウェア保護システムの動作を説明する。なお、以下の説明では、ソフト実行器１０１と注文管理器１０２との間の通信は、それらを操作している人間が電話を介して行なうものとする。

【００６２】まず、暗号化ソフトウェアの生成方法について説明する。ソフトウェアＳｏｆｔＡに対して固有の認証子ａｕｔｈＡが定められる。そして、ＳｏｆｔＡと、認証子ａｕｔｈＡとが結合され、この結合されたデータがシステム内で共通の秘密情報Ｓ（図示せず）を用いて暗号化され、暗号化ソフトウェアが生成される。式で表現すると、暗号化ソフトＥＳｏｆｔＡは、

ＥＳｏｆｔＡ＝Ｅ（Ｓ，ａｕｔｈＡ‖ＳｏｆｔＡ）
となる。なお、上式において、Ｅ（Ｓ，＊）はＳを鍵とした暗号関数を、‖は結合を示す。同様に、他のソフトウェアＳｏｆｔＢに関しても、固有の認証子ａｕｔｈＢを対応させて暗号化ソフトウェアが作成される。以下、同じような手続きで作成された複数の暗号化ソフトウェアが、例えば１枚のＣＤ－ＲＯＭに格納され、予めソフト実行器１０１に配付される。図１の実施例においては、この暗号化ソフトウェアは、暗号化ソフトウェア格納部３に格納されている。

【００６３】ソフト実行器１０１のユーザは、ソフト実行器１０１を操作することにより、暗号化ソフトウェア格納部３に格納されているソフトウェアの中から、実行することを希望するソフトウェアを指定する。例えば、ソフトウェアＡとソフトウェアＣという具合にである。応じて、注文作成部４は、対応する注文情報を生成する。この注文情報は、注文作成部４内に一旦蓄積される。そして、ソフト実行器１０１のユーザは、この注文情報と、ソフト実行器１０１に固有の実行器ＩＤ（実行器ＩＤ格納部５に格納されている）とを、注文管理器１０２のオペレータに電話で通知する。これによって、注文が完了する。

【００６４】注文管理器１０２内の実行権生成パスワード生成部１２は、ソフト実行器１０１から通知された注文情報が入力されると、まず注文を出したソフト実行器１０１の認証（または、ユーザ認証）を行ない、次に、実行器暗号キー格納部１１から該当のソフト実行器１０１の暗号キーを獲得する。次に、実行権生成パスワード生成部１２は、ソフト実行器１０１から受け取った注文情報と、実行器暗号キー格納部１１から獲得した実行器暗号キーとを結合して、この結合データを予め定められたハッシュ関数に入力する。このハッシュ関数の出力は、実行権生成パスワードとして、電話でソフト実行器１０１のユーザに伝えられる。

【００６５】ここで、ハッシュ関数は、データ圧縮型暗号処理であり、その出力が入力のすべてのビットに依存しており、出力が同じとなる異なる入力ペアを容易には見付けることができないという性質を持っている。その具体的な構成方法については、例えば池野、小山共著の「現代暗号理論」、電子通信学会発行の２２４ページから２２５ページに詳しく記述されている。なお、本実施例で用いるハッシュ関数は、例えば入力を１０進１０桁くらいの値に圧縮する関数とする。

【００６６】ソフト実行器１０１のユーザは、電話で受け取った実行権生成パスワードを、実行権生成パスワード検査部７に入力する。この実行権生成パスワード検査部７には、注文管理器１０２で用いているのと同じハッシュ関数が格納されている。そして、実行権生成パスワード検査部７は、このハッシュ関数に、注文作成部４内に蓄積されている注文情報と、実行器暗号キー格納部６内に格納されている実行器暗号キーとを結合したデータを入力する。次に、実行権生成パスワード検査部７は、このハッシュ関数の出力結果を、注文管理器１０２から得た実行権生成パスワードと比較する。このとき、注文作成部４内に蓄積されている注文情報が実際に注文管理器１０２に伝えられた内容と違っていたり、ソフト実行器１０１内に格納されている実行器暗号キーが注文管理器１０２内で獲得された実行器暗号キーと異なっている場合には、この比較結果は、ＮＧ（不一致）となる。

【００６７】実行権生成部８は、上記実行権生成パスワード検査部７での検査結果がＯＫ（一致）のときにのみ、起動されて実行権の生成を行なう。その方法は、次のとおりである。まず、実行権生成部８は、注文作成部４内に蓄積されている注文情報を参照して、対応する暗号化ソフトウェアを暗号化ソフト格納部３から取り出す。例えば、暗号化ソフトウェアとして、ＥＳｏｆｔＡを取り出したと想定すると、実行権生成部８は、この取り出した暗号化ソフトウェアＥＳｏｆｔＡを、システム内で共通の秘密鍵Ｓ（図示せず）を用いて復号し、対応する認証子ａｕｔｈＡを得る。次に、実行権生成部８は、この認証子ａｕｔｈＡを、実行器暗号キー格納部６に格納されている実行器暗号キーを用いて暗号化し、この暗号化で得た認証子を、実行権として実行権格納部９に格納する。一般的に、特定の実行器暗号キーＳｘを備えたソフト実行器Ｘの場合、ソフトＡの実行権は、Ｅ（Ｓｘ，ａｕｔｈＡ）となる。この実行権は、実行器Ｘ固有の暗号キーＳｘで暗号化されているため、実行権格納部９として、外部からの読出プロテクトが施されていない一般のメモリを用いた場合でも、機密漏洩の問題は生じない。

【００６８】ソフトウェアＡを実行する際には、ソフト復号実行部１０は、まず暗号化ソフトウェアＥＳｏｆｔＡをシステム内で共通の秘密鍵Ｓを用いて復号し、認証子ａｕｔｈＡとＳｏｆｔＡとを得る。次に、ソフト復号実行部１０は、ソフトウェアＡに対応する実行権Ｅ（Ｓｘ，ａｕｔｈＡ）を、実行権格納部９から取り出す。次に、ソフト復号実行部１０は、実行権Ｅ（Ｓｘ，ａｕｔｈＡ）を実行器暗号キーＳｘで復号して得た値と、先に得ていた認証子とを比較する。そして、ソフト復号実行部１０は、両者が一致するときに、ソフトウェアＳｏｆｔＡを実行する。

【００６９】以上説明したように、本発明の第１の実施例では、従来システムにおいて注文管理器が行なっていた実行権の生成（従来例では、暗号化ファイルキーの生成に相当する）を、ソフト実行器側で行なっている。すなわち、本実施例では、注文管理器１０２は、実行権生成部８に対して起動の許可を与えるだけの機能を有している。ここで、許可情報となる実行権生成パスワードは、注文情報と実行器の暗号キーとに依存したハッシュ関数の出力であるため、１０進１０桁程度の値で実現で

き、電話での伝え間違え、入力間違えが少なくなり、ユーザインタフェースも良好になる。また、注文情報および実行器の認証が可能となる。また、注文管理器１０２は、実行権生成部８に対し起動の許可を与えるだけなので、実行権生成パスワードは、注文するソフトの個数に依存せず、いつも少ない桁数で実現できる。

【００７０】次に、上記第１の実施例のソフトウェア保護システムにおいて、不正行為に対する安全性について説明する。第１の実施例のシステムでは、注文管理器１０２がソフト実行器１０１から注文を受けて、それに対する実行権生成パスワードを発行する際に、注文に対応した課金がなされるものとしている。支払の方法としては、一般的にはクレジット等の方法が採用されるであろう。従って、ソフト実行器１０１において、課金の対象とならない不正な実行権を勝手に生成することが困難であれば、システムの安全性が高いということになる。

【００７１】まず、不正な実行権を生成させるための外部からの攻撃として、ソフト実行器１０１内の実行権生成部８を単独で動作させることが考えられる。また、注文作成部４で作成した注文以外のソフトウェアの実行権を、実行権生成部８で作成させるという攻撃も考えられる。これらの攻撃に対しては、ユーザがソフト実行器１０１内の各構成要素を変更できないようにすることにより対処できる。

【００７２】第１の実施例では、実行権生成部８は、注文作成部４において注文が行なわれ、次にそれに対応する実行権生成パスワードの検査が通るという一連の作業を経た後でなければ起動しない。すなわち、第１の実施例では、実行権生成部８だけが単独で動作するように変更することはできない。また、第１の実施例では、上記一連の作業から注文作成を除いて、実行権生成パスワードの検査と実行権生成部８だけを動作させることもできない。さらに、注文作成部４において作成された注文情報が、実行権生成パスワード検査部７と実行権生成部８とで用いられる際、そのいずれにおいてもユーザは、注文情報の内容を変更できない。従って、第１の実施例では、上記のような不正な攻撃が行われても、実行権が生成されることはない。

【００７３】なお、ソフト実行器１０１が専用器である場合や、ソフト実行器内のプログラムがＣＤ－ＲＯＭなどで実現されている場合が非常に一般的であるということを考慮すると、ユーザがソフト実行器内の各構成要素を変更できないようにすることは、現実に即したものである。

【００７４】また、ソフトウェアを不正に実行するために、ある注文に対して受け取った実行権生成パスワードを、別の注文に対する実行権生成パスワードとして入力したり、また注文を出したソフト実行器以外のソフト実行器に入力してみるという攻撃も考えられる。ところが、第１の実施例のシステムでは、実行権生成パスワードは、注文情報と実行器暗号キーとに依存した値であるため、注文情報やソフト実行器が違う場合には、実行権生成パスワードの検査が通らない。従って、第１の実施例は、このような不正な攻撃に対しても対処できる。

【００７５】さらに、ソフトウェアを不正に実行するために、ある注文の実行権生成パスワードに対し、総当たり的に適当な値のパスワードを入力してみるという攻撃も考えられる。しかしながら、第１の実施例では、パスワードの桁数を１０進で１０桁くらいに設定しているため、不正ユーザが適当にパスワードを入力してみても、それがたまたま検査部７をパスする確率は、実際上０に近いと考えられる。従って、第１の実施例は、このような攻撃に対しても対処できる。

【００７６】さらに、ソフトウェアを不正に実行するために、ユーザが実行権生成パスワードを偽造することも考えられる。これに対しては、例えば公開鍵署名法を用いて対処することができる。公開鍵署名法を用いた場合、実行権生成パスワードを生成するためには、注文管理器１０２の秘密鍵が必要となるため、一般のユーザには、パスワードの偽造はできない。また、実行権生成パスワードを発行するための手続き（演算）を公開しないという方法でも対処できる。上記第１の実施例では、ソフト実行器２内の実行権生成パスワード検査部７は、実行権生成パスワードの生成と同じ手順で検査を行なうが、ユーザには実行権生成パスワード検査部７のアルゴリズムが公開されない。さらに、実行権生成パスワード検査部７が単独で使用する（すなわち、ソフト実行器１０１内の構成要素を変更する）ことができないため、パスワード偽造の問題は生じない。

【００７７】また、実行権格納部９を、読出プロテクト機能を持たない一般のメモリを用いて構成した場合、実行権格納部９に格納されている実行権を解析することにより、実行権を不正に生成するということも考えられる。しかしながら、第１の実施例では、実行権格納部９内に格納されている実行権は、対応するソフト実行器１０１の暗号キーで暗号化され、しかも実行器暗号キーが６４ビット程度に設定されているので、容易には実行権を解析できない。さらに、ユーザが実行器暗号キーを観察できないようにする、またはユーザに対して復号処理を公開しないようにすることで、より安全性を高めることができる。

【００７８】以上の説明により、ソフト実行器１０１側で実行権を偽造することは、事実上不可能であることが分かる。

【００７９】なお、上記第１の実施例のシステムは、ユーザが実行権を手に入れたら、その実行権を無限回数使用できるようなシステム、すなわち「実行権買い取り式」のシステムとして構成されている。従って、同じ注文情報に対する実行権生成パスワードが複数回入力されてもかまわない。

【００８０】（２）第２の実施例
図２は、本発明の第２の実施例に係るソフトウェア保護システムの構成を示すブロック図である。この第２の実施例は、第１の実施例のような「実行権買い取り式」のシステムとは異なり、ソフトウェアの実行権に例えば実行回数などの条件が付加されている場合に有効となる。
【００８１】ところで、注文したソフトウェアの実行回数を制限するためには、実行権生成パスワードは、最初の入力時にのみ有効とならなければならない。これは２回目以降の入力時にも有効であれば、次のような不都合が生じるからである。例えば、あるソフト実行器がソフトウェアＡをＮ回実行する注文を作成し、注文管理器から当該注文に対する実行権生成パスワードを手に入れたとする。ソフト実行器にこのパスワードが入力されると、ソフトウェアＡをＮ回実行できる実行権が生成される。次に、この実行権が少なくなった時点で、同じソフト実行器において再度ソフトウェアＡをＮ回実行する注文を作成し、注文管理器には注文せずに、以前のパスワードを入力する。このパスワードがもし有効となり、再度ソフトウェアＡのＮ回の実行権が生成されると、実質的に実行回数の制限は意味がなくなってしまう。
【００８２】そこで、第２の実施例では、実行権生成パスワードを最初の入力時だけ有効とするために、第１の実施例の構成に加えて、注文ごとに変化する値を導入している。すなわち、第２の実施例では、個々の注文情報に対して、その都度値が変化する変化値を生成し、この変化値に対応した実行権生成パスワードだけが有効となるようにしている。この注文ごとに変化する変化値の実現方法としては種々考えられるが、第２の実施例では、注文ごとに乱数を発生し、この乱数を注文ごと変化する変化値として用いるようにしている。
【００８３】図２において、本実施例のソフトウェア保護システムは、ソフトウェアを実行するソフト実行器２０１と、ソフト実行器２０１に対してソフトウェアを配付する注文管理器２０２とを備えている。ソフト実行器２０１は、図１の実施例と同様の構成の、暗号化ソフトウェア格納部３と、注文作成部４と、実行器ＩＤ格納部５と、実行器暗号キー格納部６と、実行権生成部８と、実行権格納部９と、ソフト復号実行部１０とを含む。さらに、ソフト実行器２０１は、注文のたびに起動する乱数生成器２０と、受け取った実行権生成パスワードの正当性を、注文情報，実行器暗号キーおよび乱数データを用いて確かめる実行権生成パスワード検査部２１とを含む。
【００８４】一方、注文管理器２０２は、図１の実施例と同様の構成の実行器暗号キー格納部１１を含む。さらに、注文管理器２０２は、ソフト実行器２０１から送付された注文情報および乱数と、実行器暗号キー格納部１１から獲得したソフト実行器２０２の暗号キーとを用いて、それらすべてに依存する実行権生成パスワードを生成する実行権パスワード生成部２２を含む。
【００８５】以上述べたように、この第２の実施例では、注文のたびに新しい乱数が生成される。そして、ソフト実行器２０１のユーザは、第１の実施例における注文情報および実行器ＩＤに加え、この乱数を、注文管理器２０２のオペレータに電話で通知する。なお、この乱数は、ユーザインタフェースを良好にするために、１０進１０桁程度の値とする。
【００８６】注文管理器２０２における実行権生成パスワード生成部２２は、第１の実施例で用いたのと同様のハッシュ関数に、注文情報，乱数および該当するソフト実行器２０１の実行器暗号キーを結合したデータを入力する。そして、このハッシュ関数の出力結果である１０進１０桁の値は、実行権生成パスワードとして、ソフト実行器２０１のユーザに電話で通知される。
【００８７】通知を受けたソフト実行器２０１のユーザは、上記実行権生成パスワードを、ソフト実行器２０１の実行権生成パスワード検査部２１に入力する。実行権生成パスワード検査部２１は、注文作成部４および乱数発生部２０から得た注文情報および乱数と、注文管理器２０２から得た実行器暗号キーとを結合して、注文管理器２０２で使用しているハッシュ関数と同様のハッシュ関数に入力する。そして、実行権生成パスワード検査部２１は、このハッシュ関数の出力結果を、入力された実行権生成パスワードと比較し、両者が一致しているときのみ、実行権生成部８を起動する。これ以降の動作は、前述した第１の実施例と同様であるので、その説明を省略する。
【００８８】上記第２の実施例では、注文のたびに新しい乱数が自動的に生成される。そして、正規の手続きの場合、注文管理器２０２からは、この乱数（＝注文ごとに変化する値）に依存した実行権生成パスワードが発行される。そして、この実行権作成パスワードは、対応する乱数を保持するソフト実行器２０１においてのみ有効となる。従って、２回目以降の注文発生時における乱数が、１回目の注文発生時に生成された乱数とは異なるため、１回目の注文発生時に得た実行権生成パスワードを、複数回不正使用することはできない。なお、第２の実施例では、第１の実施例において説明した安全性確保に対する対処に加え、上記乱数をユーザが勝手に変更したり設定できないようにすることが好ましい。
【００８９】なお、上記第２の実施例では、新しい注文が作成されるまでは、以前の乱数が残っているように構成されているが、一旦注文をセーブすることを可能とする場合には、実行権を生成した段階でそれに関与する乱数をクリアまたは更新するようにしてもよい。これによって、より一層安全性が高まる。
【００９０】（３）第３の実施例
図３は、本発明の第３の実施例に係るソフトウェア保護システムの構成を示すブロック図である。この第３の実

施例は、前述の第１の実施例に効率のよい実行器認証を付加したものである。図３において、第３の実施例のソフトウェア保護システムは、ソフトウェアを実行するソフト実行器３０１と、ソフト実行器３０１に対してソフトウェアを配付する注文管理器３０２とを備えている。

【００９１】ソフト実行器３０１は、前述の第１の実施例と同様の構成の、暗号化ソフトウェア格納部３と、注文作成部４と、実行器ＩＤ格納部５と、実行器暗号キー格納部６と、実行権生成部８と、実行権格納部９と、ソフト復号実行部１０とを含む。さらに、ソフト実行器３０１は、注文情報と実行器暗号キーに依存した注文認証情報を生成する注文認証情報生成部３０と、注文管理器３０２から受け取った実行権生成パスワードの正当性を、注文情報，実行器暗号キーおよび注文認証情報を用いて検査する実行権生成パスワード検査部３１とを含む。

【００９２】一方、注文管理器３０２は、図１の実施例と同様の構成の実行器暗号キー格納部１１を含む。さらに、注文管理器３０２は、ソフト実行器３０１から受け取った注文情報および注文認証情報と、実行器暗号キー格納部１１から獲得した実行器暗号キーとを用いてソフト実行器の認証を行なう実行器認証部３２と、実行器認証結果がＯＫの場合に、注文認証情報を注文情報を識別する注文識別情報として用い、さらに注文情報と注文識別情報（＝注文認証情報）とを用いて実行権生成パスワードを生成する実行権生成パスワード生成部３３とを含む。

【００９３】次に、図３に示す第３の実施例のソフトウェア保護システムの動作を説明する。まず、ソフト実行器３０１の注文作成部４で注文情報が作成されると、注文認証情報生成部３０は、第１の実施例で用いたのと同様のハッシュ関数に、注文情報と実行器暗号キー格納部６から得た実行器暗号キーとを結合したデータを入力する。そして、ソフト実行器３０１のユーザは、上記ハッシュ関数の出力結果を注文認証情報として、注文情報および実行器ＩＤに加えて、注文管理器３０２のオペレータに電話で伝える。なお、注文情報および注文認証情報は、それぞれ、注文作成部４および注文認証情報生成部３０に蓄積されている。

【００９４】注文管理器３０２では、まず実行器認証部３２が、ソフト実行器３０１から受け取った実行器ＩＤを鍵として、実行器暗号キー格納部１１を検索し、該当するソフト実行器３０１の実行器暗号キーを獲得する。次に、実行器認証部３２は、ソフト実行器３０１から受け取った注文情報と実行器暗号キーとを結合したデータを、ソフト実行器３０１で用いているのと同様のハッシュ関数に入力する。次に、実行器認証部３２は、このハッシュ関数の出力結果を、ソフト実行器３０１から受け取った注文認証情報と比較する。そして、実行器認証部３２は、比較結果が一致しているときのみ、相手が正しい実行器であり正しい注文を行なったものと判断し、注文認証情報を注文を識別する注文識別情報として、例えば注文情報およびこれに関連した情報の管理や授受に用いる。また、実行権生成パスワード生成部３３は、注文情報と注文識別情報（＝注文認証情報）とを結合したデータを、上記と同様のハッシュ関数に入力する。そして、注文管理器３０２のオペレータは、そのハッシュ関数の出力結果を、実行権生成パスワードとして、注文識別情報と対にしてソフト実行器３０１のユーザに電話で伝える。

【００９５】ソフト実行器３０１のユーザは、伝えられた実行権生成パスワードを、実行権生成パスワード検査部３１に入力する。応じて、実行権生成パスワード検査部３１は、注文作成部４に蓄積された注文情報と、注文認証情報生成部３０に蓄積された注文認証情報とを結合したデータをハッシュ関数に入力し、その出力結果が入力された実行権生成パスワードと一致するか否かを検査する。そして、実行権生成パスワード検査部３１は、この検査結果が一致している場合にのみ、実行権生成部８を起動する。これ以降の動作は、第１の実施例と同様であり、その説明を省略する。

【００９６】上記第３の実施例では、注文管理器３０２は、実行権生成パスワードの発行前に、注文情報およびソフト実行器の認証を行なう。実際のシステムでは、注文により課金がなされるため、いずれにせよ認証機能は必要である。この認証機能は、注文と切り離して別途設けることもできるが、例えば、チャレンジを行ないそれに対する応答により認証する方法では、これらチャレンジおよび応答のやりとりが、実際上、ソフト実行器のユーザに対してかなりの負担を与えることになる。そこで、第３の実施例では、注文情報およびソフト実行器の認証を、注文と同時に効率的に行なうようにしている。そのため、第３の実施例では、注文情報および実行器の暗号キーに依存した注文認証情報を導入している。そして、この注文認証情報は、注文情報および実行器ＩＤに加えられて、注文管理器３０２に伝えられる。なお、この注文認証情報は、上記第３の実施例ではハッシュ関数の出力であるため、例えば１０進１０桁程度で実現でき、電話で伝える場合にもそれほどユーザに負担を与えない。

【００９７】注文管理器３０２は、上記注文認証情報を用いることにより、注文情報およびソフト実行器３０１の認証を行なっている。つまり、ソフト実行器３０１が注文作成部４で作成した注文情報と、注文管理器３０２に電話で伝えた注文情報とが異なっている場合には、注文管理器３０２の実行器認証部３２において、ＮＧが出力される。また、あるソフト実行器が自分の実行器ＩＤと異なる情報を電話で伝えた場合にも、この実行器認証部３２でチェックできる。

【００９８】上記認証結果がＯＫの場合にのみ、注文管

理器３０２は、注文認証情報を注文を識別するための注文識別情報として用いる。そして、注文管理器３０２は、この注文に対応した実行権生成パスワードを生成する。この実行権生成パスワードは、ソフト実行器３０１に伝えられる。この実行権生成パスワードもハッシュ関数の出力であるため、１０進１０桁程度で実現できる。ソフト実行器３０１では、入力された実行権生成パスワードを、内部に蓄えている注文情報および注文認証情報（＝注文識別情報）を用いて検査する。この検査を経た後、入力された実行権生成パスワードに対応した注文認証情報および注文情報を保持する特定のソフト実行器でのみ有効となる実行権が生成される。なお、ここでは、実行権生成パスワードの注文識別情報（＝注文認証情報）の中に、実行器暗号キーの情報がすでに含まれているため、実行権生成パスワード自身に実行器暗号キーは含まれていない。

【００９９】上記第３の実施例では、ソフト実行器３０１のユーザは、注文時に第１の実施例で伝達すべき情報に加えて、注文認証情報を注文管理器３０２に伝えている。このことにより、注文管理器３０２は、実行権生成パスワードを発行する前に、注文情報およびソフト実行器の認証を行うことができる。この注文認証情報は、１０進１０桁程度の値であり、ソフト実行器３０１のユーザに対してそれほど負担を与えない。また、第１の実施例と同じ回数のやりとりで認証を実現でき、ユーザ認証を別途設ける場合に比べて効率がよい。そして、この注文認証情報は、注文情報を識別する注文識別情報として、注文情報やそれに関係する情報を管理するのに用いられる。

【０１００】（４）第４の実施例

図４は、本発明の第４の実施例に係るソフトウェア保護システムの構成を示すブロック図である。この第４の実施例は、乱数を導入した第２の実施例に、効率のよい実行器認証機能を付加したものである。第４の実施例も第２の実施例と同様に、例えばソフトの実行権に実行回数などの条件が付加されている場合に有効となる。図４において、第４の実施例のソフトウェア保護システムは、ソフトウェアを実行するソフト実行器４０１と、ソフト実行器４０１に対してソフトウェアを配付する注文管理器４０２とを備えている。

【０１０１】ソフト実行器４０１は、前述の第１の実施例と同様の構成の、暗号化ソフトウェア格納部３と、注文作成部４と、実行器ＩＤ格納部５と、実行器暗号キー格納部６と、実行権生成部８と、実行権格納部９と、ソフト復号実行部１０とを含む。さらに、ソフト実行器４０１は、注文情報および実行器暗号キーを結合してハッシュ演算を行う注文ハッシュ部４０と、予め定められた構造や意味をもつ乱数を注文ごとに生成する乱数生成部４１と、当該乱数および注文ハッシュ部４０の出力の排他的論理和を演算する排他的論理和部４２とを含む。

【０１０２】一方、注文管理器４０２は、図１の実施例と同様の構成の実行器暗号キー格納部１１を含む。さらに、注文管理器４０２は、実行器暗号キー格納部１１から獲得した実行器暗号キーおよびソフト実行器４０１から受け取った注文情報を結合してソフト実行器４０１と同じハッシュ演算を行う注文ハッシュ部４４と、ソフト実行器４０１から受け取った注文番号および注文ハッシュ部４４の出力の排他的論理和を演算する排他的論理和部４５と、排他的論理和部４５の出力を入力しソフト実行器４０１の正当性を認証する実行器認証部４６と、実行器認証部４６の認証結果がＯＫのときのみに起動して実行権生成パスワードを発生する実行権生成パスワード生成部４７とを含む。

【０１０３】次に、図４に示す第４の実施例のソフトウェア保護システムの動作を説明する。まず、ソフト実行器４０１において、注文作成部４が注文情報を作成すると、注文ハッシュ部４０は、第１の実施例で用いたのと同様のハッシュ関数に、当該注文情報と実行器暗号キー格納部６から得たソフト実行器の暗号キーとを結合したデータを入力する。また、乱数生成部４１は、予め定められた構造や意味を持った乱数データを生成する。一例として、本実施例では、乱数データの最上位から３ビットを“０”とし、最下位から３ビットを“１”としている。その他のビットは乱数を格納する。この例の他、注文管理器４０２とソフト実行器４０１との間で予め取り決めしておいて、その乱数データのある部分に、実行器ＩＤの一部のデータを対応させてもよい。次に、排他的論理和部４２は、注文ハッシュ部４０の出力と、乱数生成部４１で生成された乱数データとの排他的論理和を演算する。ソフト実行器４０１のユーザは、この排他的論理和部４２の演算結果を注文認証情報として、注文情報および実行器ＩＤと共に、注文管理器４０２のオペレータに伝える。なお、上記乱数データのビット数を、注文ハッシュ部４０の出力と同程度にとれば、注文認証情報は１０進１０桁程度となり、ソフト実行器４０１のユーザや注文管理器４０２のオペレータにそれほど大きな負担を与えない。

【０１０４】注文管理器４０２では、実行器認証部４６が実行器暗号キー格納部１１から該当するソフト実行器の暗号キーを獲得し、これと注文情報とを結合して注文ハッシュ部４４に入力する。そして、排他的論理和部４５は、注文ハッシュ部４４の出力と、ソフト実行器４０１から受け取った注文認証情報との排他的論理和を演算する。注文情報と実行器ＩＤとが正しければ、注文ハッシュ部４４の出力は、注文を行ったソフト実行器４０１内の注文ハッシュ部４０の出力と同じになる。また、排他的論理和部４５の出力は、注文を行ったソフト実行器４０１の乱数生成部４１で生成した乱数データと同じになる。つまり、今の場合、乱数データの最上位から３ビットは“０”、最下位から３ビットは“１”となる。実

行器認証部４６は、排他的論理和部４５の出力が、予め定められている乱数の構造や意味を持っているか否かを確認し、ＯＫであれば、注文情報と実行器とが正しいと認証する。そして、この認証結果がＯＫの場合にのみ、実行権生成パスワード生成部４７は、実行権生成パスワードを生成する。これ以降の動作は、第３の実施例と同じである。すなわち、注文管理器４０２で生成された実行権生成パスワードが、電話等によってソフト実行器４０１に伝えられ、ソフト実行器側でそれを検査して、ＯＫの場合に対応するソフトの実行権が作成される。

【０１０５】上記第４の実施例では、第２の実施例と同様に、乱数を導入して回数制限付きの実行権生成に対応できる。さらに、第４の実施例は、第３の実施例と同様に、ユーザ認証機能を備えている。このように第４の実施例は、第２および第３の実施例の機能を併せ持つにもかかわらず、ソフト実行器４０１と注文管理器４０２間でやり取りするデータ量、特にランダムな注文番号と実行権生成パスワードの桁数が増加していない。

【０１０６】（５）第５の実施例

図５は、本発明の第５の実施例に係るソフトウェア保護システムの構成を示すブロック図である。この第５の実施例では、各ソフト実行器内に不活性状態の実行権生成モジュールが備えられており、注文管理器から与えられる実行権生成パスワードによりその実行権生成モジュールを活性化させて、そのモジュールで所定の実行権を生成することを特徴としている。なお、以下の説明では、実行権生成モジュールが２つの部分に分けられ、その一方である実行権生成モジュールＡがソフト実行器に蓄えられ、もう一方の実行権生成モジュールＢは、暗号化されてソフト実行器が注文管理器から受け取る。この実行権生成モジュールＡおよびＢは、両者が揃って初めて所定の実行権が生成できる。従って、ソフト実行器内に蓄えられた実行権生成モジュールＡだけでは不活性な状態であり、実行権を生成できない。

【０１０７】図５において、第５の実施例のソフトウェア保護システムは、ソフトウェアを実行するソフト実行器５０１と、ソフト実行器５０１に対してソフトウェアを配付する注文管理器５０２とを備えている。

【０１０８】ソフト実行器５０１は、前述の第１の実施例と同様の構成の、暗号化ソフトウェア格納部３と、注文作成部４と、実行器ＩＤ格納部５と、実行器暗号キー格納部６と、実行権生成部８と、実行権格納部９と、ソフト復号実行部１０とを含む。さらに、ソフト実行器５０１は、注文情報および実行器暗号キーを結合してハッシュ演算を施す注文ハッシュ部５０と、実行権生成モジュールＡを格納する格納部５１と、注文管理器５０２から受け取った実行権生成パスワードを逆変換する逆変換部５２と、逆変換部５２の逆変換結果を格納する格納部５３とを含む。なお、注文情報と実行器ＩＤとが正しければ、この格納部５３には、実行権生成モジュールＢが格納されることになる。

【０１０９】一方、注文管理器５０２は、図１の実施例と同様の構成の実行器暗号キー格納部１１を含む。さらに、注文管理器５０２は、ソフト実行器５０１から受け取った注文情報と、実行器暗号キー格納部１１から得た該当の実行器の暗号キーとを結合してハッシュ演算を施す注文ハッシュ部５４と、実行権生成モジュールＢを格納する格納部５５と、モジュールＢを注文ハッシュ部５４の出力を用いて変換し、実行権生成パスワードを生成する実行権生成パスワード生成部５６とを含む。

【０１１０】次に、図５に示す第５の実施例のソフトウェア保護システムの動作を説明する。まず、ソフト実行器５０１のユーザは、ソフト実行器５０１を操作することにより、実行を希望するソフトウェアの注文を指定する。応じて、注文作成部４は、対応する注文情報を作成する。そして、当該ユーザは、注文情報とソフト実行器５０１に固有の実行器ＩＤとを、電話等によって注文管理器５０２に通知する。

【０１１１】ソフト実行器５０１からの通知を受け取ると、注文管理器５０２では、実行器ＩＤに基づいて実行器暗号キー格納部１１を検索し、該当するソフト実行器の暗号キーを獲得する。次に、注文ハッシュ部５４は、ソフト実行器５０１から受け取った注文情報と、実行器暗号キー格納部１１から得た実行器暗号キーとを結合して、第１の実施例で用いたのと同様のハッシュ関数に入力する。実行権生成パスワード生成部５６は、注文ハッシュ部５４から出力されるハッシュ値を鍵として、実行権生成モジュールＢを変換し、実行権生成パスワードを発行する。注文管理器５０２のオペレータは、この実行権生成パスワードを、電話等によってソフト実行器５０１のユーザに伝える。

【０１１２】次に、電話で実行権生成パスワードを受け取ったソフト実行器５０１のユーザは、ソフト実行器５０１の逆変換部５２に、このパスワードを入力する。注文ハッシュ部５０には、注文管理器５０２で用いたのと同じハッシュ関数が備えられている。そして、注文ハッシュ部５０は、注文作成部４内に蓄積された注文情報と、実行器暗号キー格納部６から得た実行器暗号キーとを結合し、この結合データに対してハッシュ演算を施す。逆変換部５２は、注文ハッシュ部５０から出力されるハッシュ値を鍵として、注文管理器５０２から受け取った実行権生成パスワードを逆変換する。もし、注文情報と実行器暗号キーとが正当であるならば、注文ハッシュ部５０から出力されるハッシュ値は、注文管理器５０２におけるハッシュ値（注文ハッシュ部５４の出力）と同じになる。従って、逆変換部５２の出力は、実行権生成モジュールＢとなる。次に、実行権生成部８は、予め格納部５１に格納されている実行権生成モジュールＡと、獲得したモジュールＢとを用いて、注文情報に対応した実行権を生成する。実行権生成部８によって実行権

が生成された後は、実行権生成モジュールに従って、モジュールＢが削除される。

【０１１３】上記第５の実施例では、ソフト実行器側に予め格納されている実行権生成モジュールＡは、不活性な状態であり、情報量的にこれだけでは動作できない。これを活性化するためのモジュールＢは、注文管理器５０２において、ソフト実行器の注文情報と暗号キーとに依存した形に変換され、実行権生成パスワードとして送付される。前述した第１～第４の実施例においては、実行権生成モジュールは、完全な形でソフト実行器内に存在した。ただし、これを起動するためには、実行権生成パスワードという許可が必要であった。これに対して第５の実施例の構成では、実行権生成モジュールは、情報量的に不足した状態でソフト実行器内に存在する。このため、第５の実施例は、第１～第４の実施例に比べて、より実行権の不正生成に対する安全性が高い。なお、実行権生成モジュールＡおよびＢにより注文の実行権を生成した後は、元の状態に戻すために、モジュールＢが削除される。

【０１１４】第５の実施例において、実行権生成モジュールＢは、注文情報と実行器の秘密キーとに依存して変換されるため、注文が異なったり実行器が異なる場合には、ソフト実行器のユーザは、正規のモジュールＢを手に入れることができない。ただし、第５の実施例では、実行権生成パスワードの中にモジュールＢが情報として含まれるため、許可情報だけが含まれていた第１～第４の実施例に比べて、多少実行権生成パスワードの桁数を増やす必要がある。なお、この第５の実施例における実行権生成パスワードのデータ量は、注文するソフトの個数に依存しない。

【０１１５】なお、第５の実施例では、ソフト実行器５０１は、注文管理器５０２から受け取った実行権生成パスワードをチェックすることなしに、逆変換後すぐにこれをモジュールＢとして用いている。従って、もし注文情報や実行器暗号キーが、入力した実行権生成パスワードに適合しない場合には、実行権生成モジュールが正しく動作しない。ところで、例えばモジュールＢがある特定の構造や意味を持っているとし、ソフト実行器５０１において逆変換後、これを使用する前に構造や意味をチェックすることも考えられる。例えば、モジュールＢがある命令コードの場合には、そのコードには特定の構造があるはずである。従って、モジュールＢがこの特定の構造を有しているか否かをチェックすることにより、実行権生成モジュールの実行前にエラーを処理することができる。

【０１１６】なお、以上述べた第２および４の実施例において用いられる乱数は、注文ごとに変化する値であれば良く、カウンタなどを用いて発生してもよい。また、乱数に代えて、タイムスタンプを用いてもよい。タイムスタンプは、ソフト実行器と注文管理器とで共通に発生可能（時計回路によって発生可能）であるため、ソフト実行器から注文管理器に対して変化値を送付する必要がなくなる。

【０１１７】また、第３および４の実施例において、実行権生成パスワードを生成する際、注文情報および注文識別情報に加えて、実行器暗号キーにも依存させるようにしてもよい。ソフト実行器にとって、自分の実行器暗号キーを知っているのは、自分以外には注文管理器だけなので、この実行権生成パスワードを作ることができるのは、注文管理器だけである。そのため、実行権生成パスワードを注文管理器の署名情報として考えることができ、トラブル等が生じたときに、この情報を第３者に証拠として提出することができる。また、このような秘密鍵暗号を用いた署名方法に代えて、公開鍵暗号を用いた署名方法を用いてもよい。この場合、注文管理器は秘密の情報を保持し、実行権生成パスワードの生成の際にこの秘密の情報を用いる。一方、ソフト実行器側では、注文管理器の秘密情報に対応する公開情報を保持しており、これを用いて実行権生成パスワードの正当性を確認する。注文管理器の秘密情報を用いた場合にのみ、実行権生成パスワードの正当性が確認できるため、この実行権生成パスワードを注文管理器の署名として考えることができる。

【０１１８】また、第１～４の実施例においては、元のソフトウェアＳｏｆｔＡと、対応する認証子ａｕｔｈＡとを結合し、この結合されたデータをシステム共通の鍵Ｓで暗号化することにより、ソフトウェアの暗号化を行うようにしていたが、また、この認証子を実行器暗号キーＳｘで暗号化したデータを実行権として用いるようにしていたが、本発明はこのような方法には限定されない。例えば、認証子と実行器ＩＤとを結合し、この結合されたデータをシステム共通の鍵で暗号化したものを、実行権として用いてもよい。実行器Ｘの実行権を、式で記述すると、

Ｅ（Ｓ，ａｕｔｈＡ　‖　ＩＤｘ）

となる。この場合、実行権は、実行権と暗号化ソフトウェアとをシステム共通の鍵で復号し、両者から得られる認証子が一致しており、かつ、実行権の復号結果から実行器ＩＤを獲得して、これが実行器内の実行器ＩＤと一致している場合に認証され、ソフトウェアを実行する。いずれにせよ、暗号化ソフトウェアから実行器がすでに保持しているデータを用いて、実行権が生成できる暗号方式ならば、本発明を適用できる。

【０１１９】また、上記第１～４の実施例においては、電話の１通話で注文を行ない、それに対する実行権生成パスワードを受け取るとしていたが、これが別の通話であってもよい。つまり、まずソフト実行器から注文管理器に対して注文を行ない、この注文を一旦セーブする。次に、注文管理器がソフト実行器に電話をかけてきて、注文番号で照合を行ない実行権生成パスワードの通知を

行なう。このことにより、ソフト実行器のユーザにとり、電話をかけている時間が短くなり、料金的にも都合がよい。また、ソフト実行器のユーザは、注文管理器のユーザから実行権生成パスワードが通知されるまで、別のソフト実行等の作業を行なうことができる。一方、注文管理器にとっても、コールバックを行なうことによってユーザ認証が行なえる。

【０１２０】また、上記第１～４の実施例において、ソフト実行器が実行権生成パスワードを検査して実行権を生成する場合には、予めセーブしておいた注文情報をロードして用いる。ただし、注文情報を再ロードし、パスワードを再度使われないようにするために、最初に実行権を生成した後、セーブしておいた注文情報を消去することが必要となる。

【０１２１】また、上記各実施例において、ソフト実行器と注文管理器とのやり取りの履歴を、双方で残しておくことにより、注文に関するトラブル時の参考資料にすることが考えられる。また、ソフト実行器側には、例えば今までどんなソフトを購入したかを残しておくことにより、注文ガイダンスのユーザインタフェースを良好なものにすることができる。

【０１２２】また、上記各実施例において、ソフト実行器から注文管理器への注文情報としては、例えばソフトＡとソフトＢという具合にソフトのＩＤを用いることにしていたが、この部分をコード化して、対応するソフト名とコードの対応表を用いることにより、より通信情報量の削減を行なうことも考えられる。つまり、ソフトＡとソフトＢならばコード２番、ソフトＢだけならばコード１０番といった具合いにである。

【０１２３】また、上記各実施例では、ソフト実行器と注文管理器との間の情報のやりとりは、人間が電話を介して行うものとして説明したが、両者に送受信器を設け、通信路を介して情報の授受を行うようにしてもよい。

【０１２４】

【発明の効果】請求項１の発明によれば、ソフト実行器は、注文に対応した正規の実行権生成パスワードを入力することによってのみソフトの実行権を生成する。そして、注文管理器からソフト実行器には、実行権生成パスワード、すなわちソフト実行器が注文情報に対応したソフト実行権を生成するための許可を与える情報だけが送付されるため、安全性を劣化させることなく、送付すべき情報量を大幅に削減することができる。また、実行権生成パスワードの情報量は、注文するソフトの個数に依存せずに、いつも少ない情報量で実現できる。すなわち、ソフト実行器が複数のソフトウェアの注文を１回に行なっても、その情報量は１つのソフトウェアを注文したの場合の情報量と同じになる。この情報量の削減により、特に電話でパスワードを送受信する場合、ユーザインタフェース的に都合がよい。また、注文管理器にとっては伝え間違えが少なくなる。またソフト実行器のユーザにとっては、聞き間違えおよびこれを実行器に入力する際に間違えが少なくなる。また、電話をつないでいる時間も削減できるため、料金的にもメリットがある。

【０１２５】請求項２，５，８，１０および１５の発明によれば、データ圧縮関数を用いて実行権生成パスワードを生成するようにしているので、その情報量をより一層削減することができる。

【０１２６】請求項３の発明によれば、ソフト実行器には、デジタル署名された実行権生成パスワードが送付されるので、ソフト実行器側で実行権生成パスワードを偽造することがほとんど不可能となり、極めて安全性の高いソフトウェア保護システムを実現することができる。

【０１２７】請求項４の発明によれば、注文情報を作成する毎に変化する変化値を導入し、注文管理器からの実行権生成パスワードは、対応する変化値を保持するソフト実行器でのみ有効となるように構成されているため、異なる時期に同じ注文を作成し、以前の実行権生成パスワードを入力しても、後の注文時に生成される変化値は、以前の注文時に生成される変化値とは異なっており、入力したパスワードが有効にはならない。これによって、例えば実行の回数が制限されているような実行権が生成される場合、実行権生成パスワードを繰り返して用いるという不正を防止することができる。

【０１２８】請求項６の発明によれば、異なる時期になされた注文を峻別するために、ソフト実行器と注文管理器とに共通に保持されているタイムスタンプを用いているので、ソフト実行器から注文管理器に峻別のための情報を送付する必要がない。

【０１２９】請求項７の発明によれば、ソフト実行器側で注文情報および実行器秘密情報に依存した注文認証情報を生成し、注文管理器に送付するようにしているので、注文管理器側で実行権生成パスワードの発行に先だって、注文情報とソフト実行器の認証を行うことができる。注文情報とソフト実行器の認証は、実際上は課金に関係するため、必要不可欠な機能である。本発明では、注文と同時にソフト実行器から少ない桁数の注文認証情報を通知することによって、効率的にこの機能を実現している。また、注文認証情報を、注文を識別する注文識別情報としても用いることができる。

【０１３０】請求項９の発明によれば、ソフト実行器と注文管理器間でやりとりされる情報の量を増やすことなく、回数制限機能およびユーザ認証機能の両方を実現することができる。

【０１３１】請求項１２の発明によれば、注文管理器からソフト実行器には、デジタル署名された実行権生成パスワードが送付されるので、ソフト実行器側で実行権生成パスワードを偽造することがほとんど不可能となり、極めて安全性の高いソフトウェア保護システムを実現することができる。

【０１３２】請求項１３の発明によれば、ソフト実行器側に格納された第２の実行権生成モジュールを活性化させるための第１の実行権生成モジュールを注文管理器に格納し、この第１の実行権生成モジュールを実行権生成パスワードに含めて送付するようにしているので、ソフト実行器側では、不正に実行権を生成しようとしても、情報量的に不足しているため、正しい実行権を生成することができない。従って、より一層安全なソフトウェア保護システムを実現することができる。

【０１３３】請求項１７の発明によれば、ソフト実行器は、作成した注文情報を不揮発的に蓄積保持し、対応するソフトウェアの実行権を生成した後に当該注文情報を消去するようにしているので、とりあえず注文だけを連続して送付し、後に返送されてくる実行権生成パスワードに基づいて、ソフトウェアの実行を制御することができる。

【０１３４】請求項１８の発明によれば、ソフト実行器および注文管理器は、それぞれ相互間でやりとりされた情報の履歴を保持しているので、後に生じるトラブル等に柔軟に対処することができる。

【０１３５】請求項１９の発明によれば、ソフト実行器および注文管理器は、すべてのソフトウェアの組み合わせに対応するコードをテーブルとして保持しており、ソフト実行器は、テーブルから得たコードを、注文情報として注文管理器に送付するようにしているので、注文情報のデータ量をより一層削減することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施例に係るソフトウェア保護システムの構成を示すブロック図である。

【図２】本発明の第２の実施例に係るソフトウェア保護システムの構成を示すブロック図である。

【図３】本発明の第３の実施例に係るソフトウェア保護システムの構成を示すブロック図である。

【図４】本発明の第４の実施例に係るソフトウェア保護システムの構成を示すブロック図である。

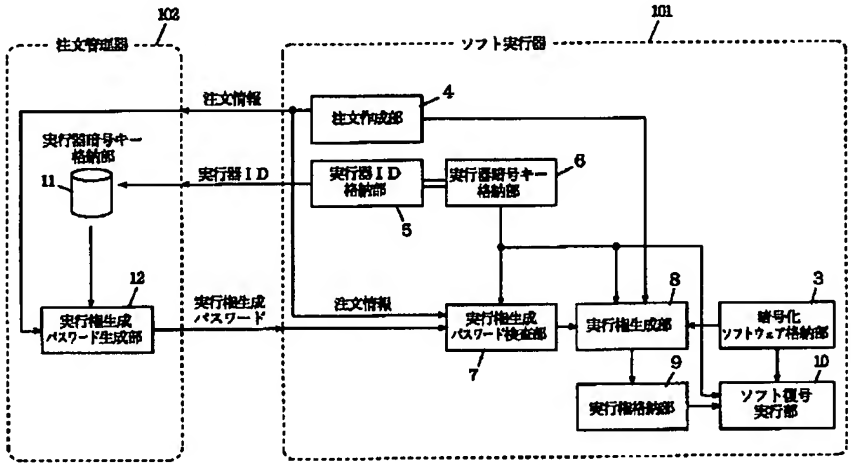
【図５】本発明の第５の実施例に係るソフトウェア保護システムの構成を示すブロック図である。

【図６】従来のソフト保護システムの構成を示すブロック図である。

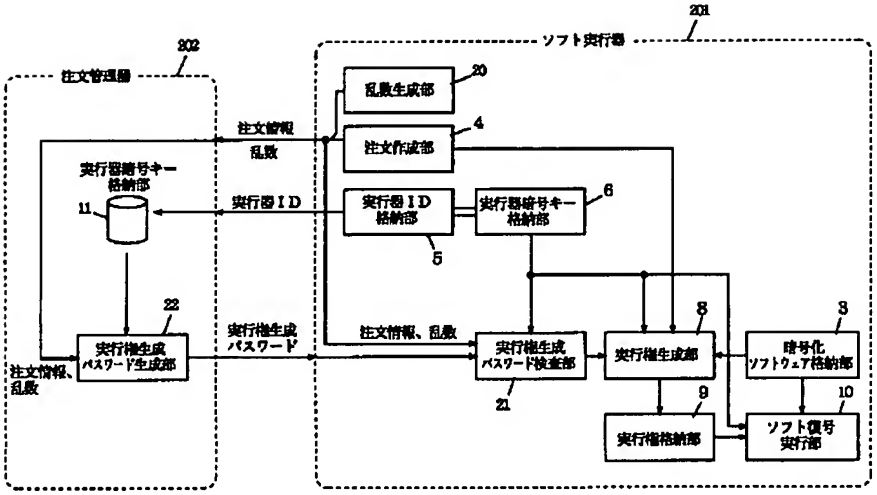
【符号の説明】

１０１～５０１…ソフト実行器
１０２～５０２…注文管理器
３…暗号化ソフトウェア格納部
４…注文作成部
５…実行器ＩＤ格納部
６…実行器暗号キー格納部
７、２１、３１、４３…実行権生成パスワード検査部
８…実行権生成部
９…実行権格納部
１０…ソフト復号実行部
１１…実行器暗号キー格納部
１２、２２、３３、４７…実行権生成パスワード生成部
２０…乱数生成部
３０…注文認証情報生成部
３２…実行器認証部
４０、４４、５０、５４…注文ハッシュ部
４２、４５…排他的論理和部
４６…実行器認証部
５１…実行権生成モジュールＡ格納部
５２、５５…実行権生成パスワード逆変換部
５３…実行権生成モジュールＢ格納部
５６…実行権生成パスワード生成部

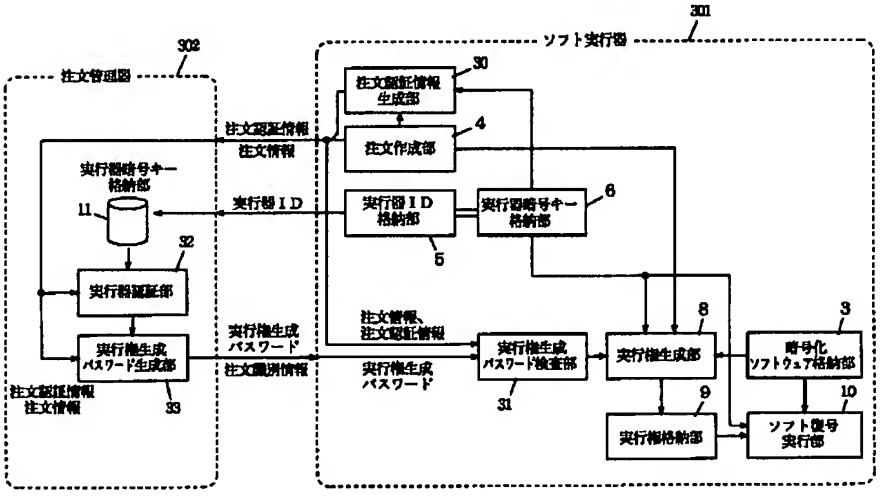
【図１】



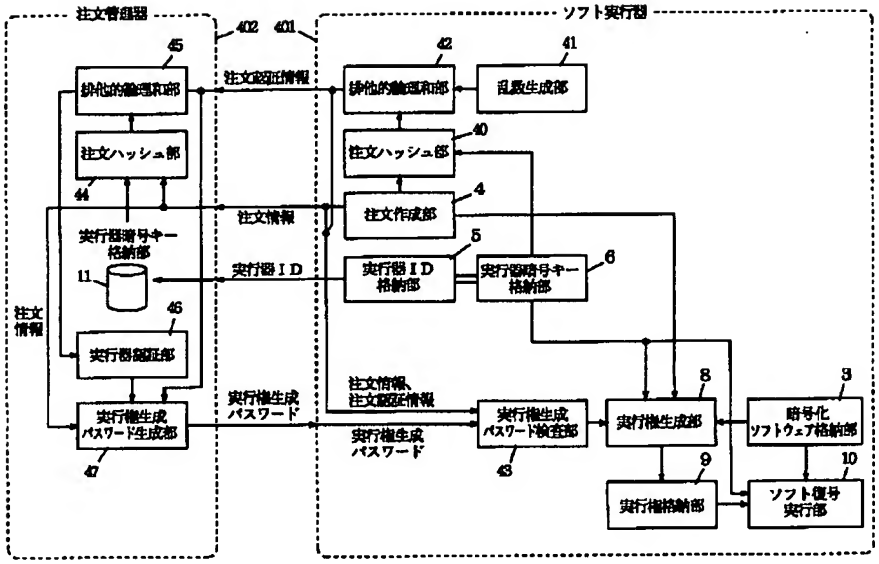
【図２】


201
ソフト実行器
202
注文管理器
乱数生成部
20
注文情報
乱数
注文作成部
4
実行器暗号キー
格納部
11
実行器ＩＤ
実行器ＩＤ
格納部
5
実行器暗号キー
格納部
6
22
実行権生成
パスワード生成部
実行権生成
パスワード
注文情報、乱数
注文情報、乱数
実行権生成
パスワード検査部
21
実行権生成部
8
3
暗号化
ソフトウェア格納部
9
10
実行権格納部
ソフト復号
実行部

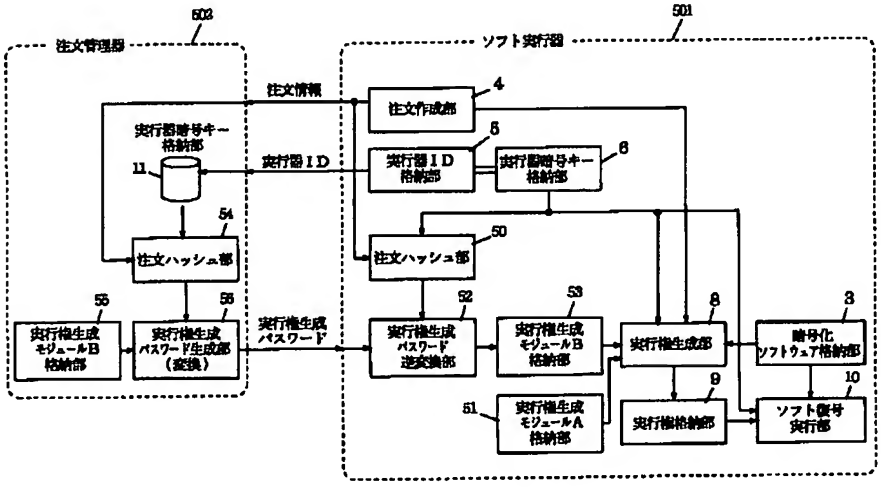
【図３】


301
ソフト実行器
302
注文管理器
注文認証情報
生成部
30
注文認証情報
注文情報
注文作成部
4
実行器暗号キー
格納部
11
実行器ＩＤ
実行器ＩＤ
格納部
5
実行器暗号キー
格納部
6
32
実行器認証部
実行権生成
パスワード
注文識別情報
実行権生成
パスワード生成部
33
注文認証情報
注文情報
注文情報、
注文認証情報
実行権生成
パスワード
実行権生成
パスワード検査部
31
実行権生成部
8
3
暗号化
ソフトウェア格納部
9
10
実行権格納部
ソフト復号
実行部

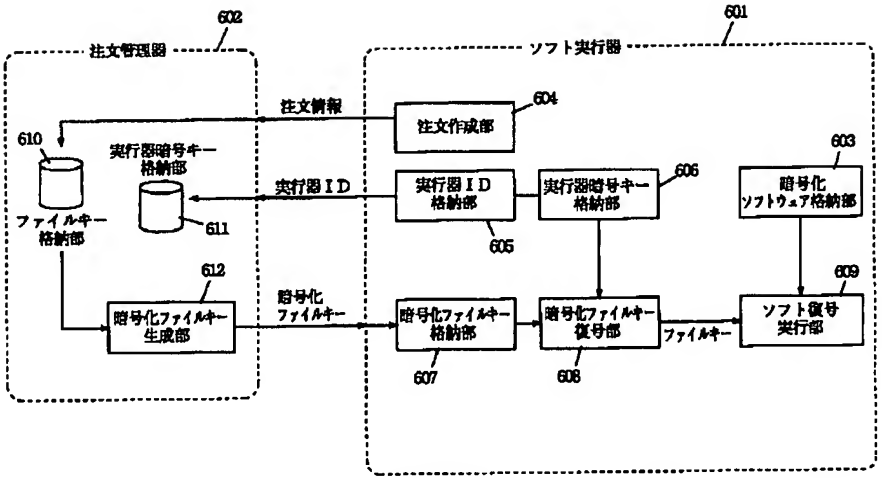
【図4】


注文管理器
402
401
ソフト実行器
45
排他的論理和部
注文認証情報
42
排他的論理和部
41
乱数生成部
注文ハッシュ部
40
注文ハッシュ部
44
4
注文作成部
注文情報
実行器暗号キー格納部
11
実行器ＩＤ
5
実行器ＩＤ格納部
実行器暗号キー格納部
6
注文情報
46
実行器認証部
注文情報、注文認証情報
8
3
実行権生成パスワード
実行権生成パスワード生成部
実行権生成パスワード
実行権生成パスワード検査部
実行権生成部
暗号化ソフトウェア格納部
47
43
9
10
実行権格納部
ソフト復号実行部

【図5】


502
501
注文管理器
ソフト実行器
注文情報
4
注文作成部
実行器暗号キー格納部
11
実行器ＩＤ
5
実行器ＩＤ格納部
実行器暗号キー格納部
6
54
50
注文ハッシュ部
55
56
52
53
8
3
実行権生成モジュールB格納部
実行権生成パスワード生成部（変換）
実行権生成パスワード
実行権生成パスワード逆変換部
実行権生成モジュールB格納部
実行権生成部
暗号化ソフトウェア格納部
9
10
51
実行権生成モジュールA格納部
実行権格納部
ソフト復号実行部

【図６】


602
注文管理器
601
ソフト実行器
注文情報
604
注文作成部
610
実行器暗号キー
格納部
実行器ＩＤ
603
暗号化
ソフトウェア格納部
実行器ＩＤ
格納部
606
実行器暗号キー
格納部
ファイルキー
格納部
611
605
612
609
暗号化
ファイルキー
暗号化ファイルキー
生成部
暗号化ファイルキー
格納部
暗号化ファイルキー
復号部
ファイルキー
ソフト復号
実行部
607
608